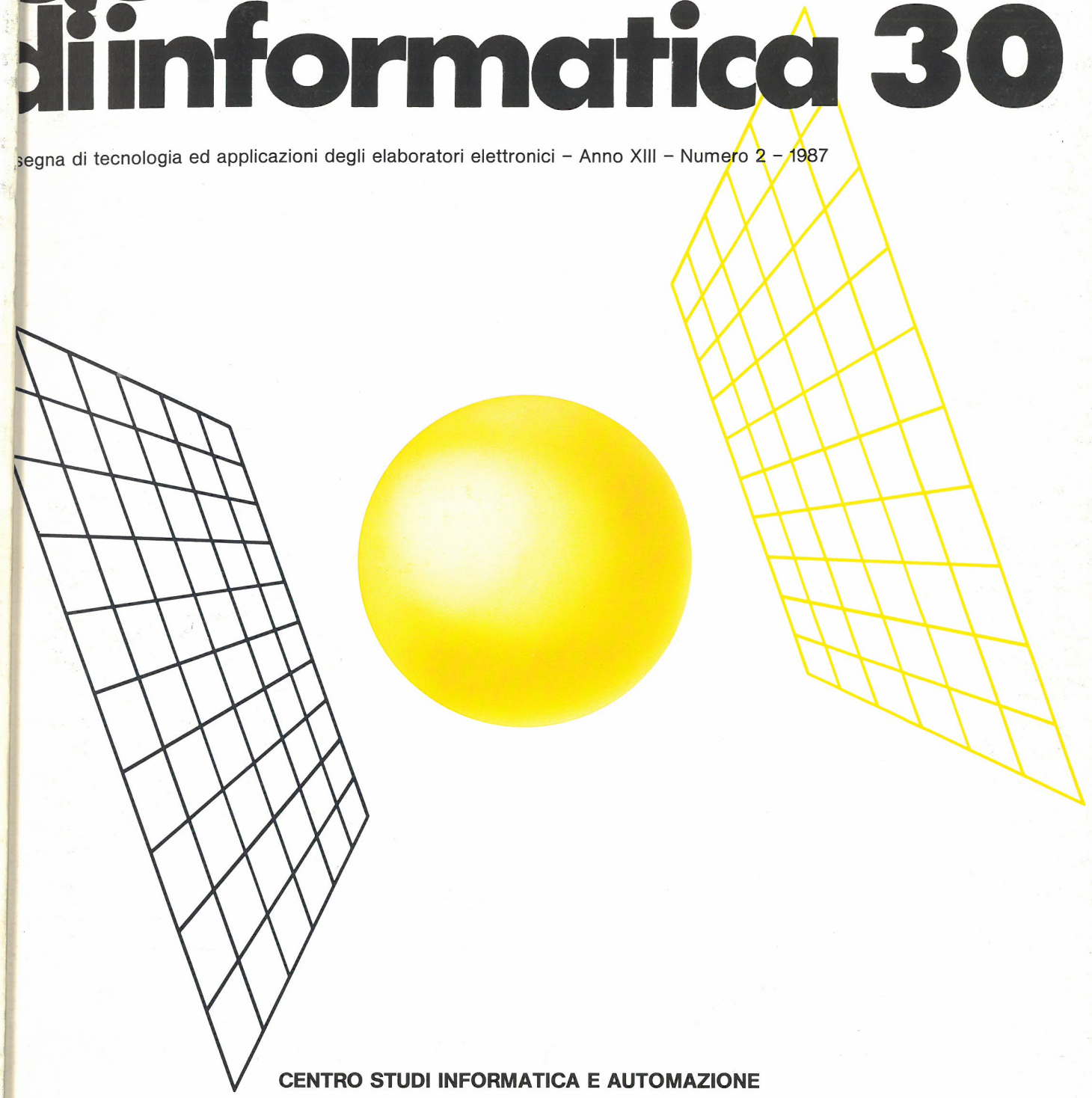
Quaderni di informatica 30

segna di tecnologia ed applicazioni degli elaboratori elettronici – Anno XIII – Numero 2 – 1987



CENTRO STUDI INFORMATICA E AUTOMAZIONE

ARCHIVIO STORICO
ASSOCIAZIONE POZZO DI MIELE
FPDM-37
RQDI 128

Honeywell Bull

Quaderni di informatica

Rassegna di tecnologia ed applicazioni degli elaboratori elettronici

Anno XIII - Numero 2 - 1987

Sommario

Informatica e cicli economici

Gli economisti hanno evidenziato l'andamento ondulatorio dei fenomeni economici nell'era moderna, correlandolo al succedersi delle innovazioni tecnologiche. Nell'articolo, l'autore riprende queste teorie, sottolineando il ruolo dell'informatica nella fase attuale.

R. LEVRERO

Un sistema esperto per la diagnosi degli elaboratori

I sistemi esperti cominciano a trovare applicazione pratica nei settori più diversi. L'articolo descrive un sistema che, sulla base della conoscenza desunta da esperti umani, assiste il tecnico nella ricerca dei guasti di una famiglia di elaboratori.

F. TORQUATI

La crittografia a chiave pubblica

La diffusione dei sistemi telematici pone con sempre maggior evidenza il problema di salvaguardare la riservatezza delle informazioni. Tra i vari metodi proposti, quello qui illustrato sembra quello ottimale.

R. BORTOLAMEAZZI, L. FELICIAN, L. SABBADINI.

Didattica col computer: una sperimentazione

Attraverso uno specifico sviluppo, gli autori intendono mostrare come, mediante un opportuno approccio concettuale, sia possibile valorizzare le potenzialità del computer quale strumento didattico.

G. CANEPA, G. GARAVAGLIA

Direttore Responsabile
Franco Filippazzi

Comitato di Redazione
A. Cicu, C. Falcetti, P. Lupo,
M. Nobile, G. Occhini
F. Sala

Redazione
Honeywell Bull
Centro Studi Informatica e Automazione
Via G.M. Vida, 11 - 20127 Milano

Stampa
tipolito Maggioni s.a.s.

Autorizzazione del Tribunale di Milano
n. 93 del 20 Marzo 1974

«Quaderni di Informatica» ospita articoli e contributi di varia provenienza. La responsabilità delle opinioni espresse rimane agli Autori.

La riproduzione di articoli della rivista, o di parte di essi, è consentita solo citando la fonte e l'autore.

Informatica e cicli economici

RENATO LEVRERO

Honeywell Bull
Direzione Pianificazione Marketing
Milano

1. Introduzione

Obiettivo di questo articolo è dare elementi quantitativi per valutare il ruolo che sta avendo l'industria informatica nell'ambito di un visione di lungo periodo dello sviluppo economico del mondo occidentale, di quell'insieme di paesi, cioè, caratterizzati dall'esistenza di una economia di mercato.

Lo scenario al quale ci riferiamo è la moderna teoria dei cicli economici quale è stata formulato nel XX secolo inizialmente dagli olandesi van Gelderns e de Wolf (negli anni '10), per poi accedere ad una duratura, seppur incostante, fortuna politica ed accademica col grande economista sovietico Kondratieff negli anni '20, ripresa poi dall'economista austro-americano Schumpeter alla fine degli anni '30, per conoscere un non banale revival negli anni '70 da parte di Rostow, Forrester (che ha coniugato teoria dei sistemi con onde lunghe), Wallerstein e Maddison.

La ripresa della teoria in tempi recenti è ovviamente dovuta alla necessità, da più parti avvertita, di rispondere alla domanda "dove stiamo andando", domanda che è stata formulata in maniera piuttosto angosciosa a partire dalla "crisi energetica" del '73 e che, dopo 15 anni, non sembra ancora aver trovato una tranquillizzante risposta.

2. La teoria dei cicli economici.

In una serie di articoli pubblicati nei primi anni '20, Kondratieff ritenne di aver individuato, analizzando indicatori economici quali i prezzi, le rendite, i valori fisici della produzione, una serie di regolarità nell'ambito delle economie dei paesi occidentali (Inghilterra, Francia, Germania), regolarità che si identificavano in una serie di picchi (tre) nell'indice dei prezzi, distanziati fra loro di un intervallo di tempo fra i 40 ed i 60 anni. Kondratieff identificava due cicli e mezzo di "onde lunghe" - a partire dal 1780 - caratterizzate fondamentalmente dall'andamento della spesa del capitale fisso (ferrovie, apertura di nuovi territori alla colonizzazione, ecc.), nonché dall'andamento complementare e in contro-fase tra i prezzi agricoli (e delle materie prime) e quelli industriali. Pur senza soffermarvisi molto, Kondratieff accenna ad un problema che costituirà il centro dell'analisi di Schumpeter vent'anni dopo: nella fase di declino si verificherebbe un'accentrarsi di innovazioni tecnico-scientifiche che sarebbero, poi, pienamente sviluppate ed applicate nella fase successiva di crescita.

Ed è precisamente Schumpeter che nel suo lavoro del 1939 integra la teoria dei cicli con quella dell'innovazione e dell'imprenditore.

Secondo Schumpeter le fasi di crescita sono scandite dalla successione di "onde" di innovazioni, - originatesi nel precedente periodo di "depressione" - quali, per il periodo del primo Kondratieff (fase di crescita: 1780-1810; fase di declino: 1817-1850) quelle dell'industria del cotone e del ferro, mentre per il secondo Kondratieff (crescita: 1844-1870; declino, 1870-1896) elemento portante sarebbe stato lo sviluppo delle ferrovie (basato sull'unione delle tecnologie derivanti dallo sfruttamento della macchina a vapore e della produzione dell'acciaio).

L'emergere dell'industria dell'elettricità e le applicazioni del motore a combustione interna (auto) sono poi le caratteristiche del terzo Kondratieff che avrebbe occupato il primo cinquantennio del XX secolo.

Le ricostruzioni di Kondratieff e Schumpeter sono affascinanti, seppure fondamentali obiezioni sono state mosse - sia dal punto di vista statistico che da quello della individuazione dei nessi di causalità fra le diverse componenti del ciclo - alle loro teorie; ciò che è importante sottolineare è che ambedue gli autori ci hanno dato una visione generale di trasformazione di una società, quella capitalistica, per l'appunto. Seppure da due punti di vista totalmente opposti - socialista l'uno, borghese l'altro - gli autori evidenziano concordemente il susseguirsi di periodi di guerre e rivoluzioni (nelle fasi di crescita del ciclo) e di pace e di "decadenza" nel periodo di crisi.

G. Imbert nel 1956 ha stabilito in modo abbastanza univoco l'esistenza di correlazioni - dal punto di vista statistico - fra le onde dei prezzi e quelle della produzione, dando così una base piuttosto sicura all'intera teoria. W. Rostow, proseguendo gli studi a livello mondiale effettuati da Kuznetz, ha formalizzato la sua in-

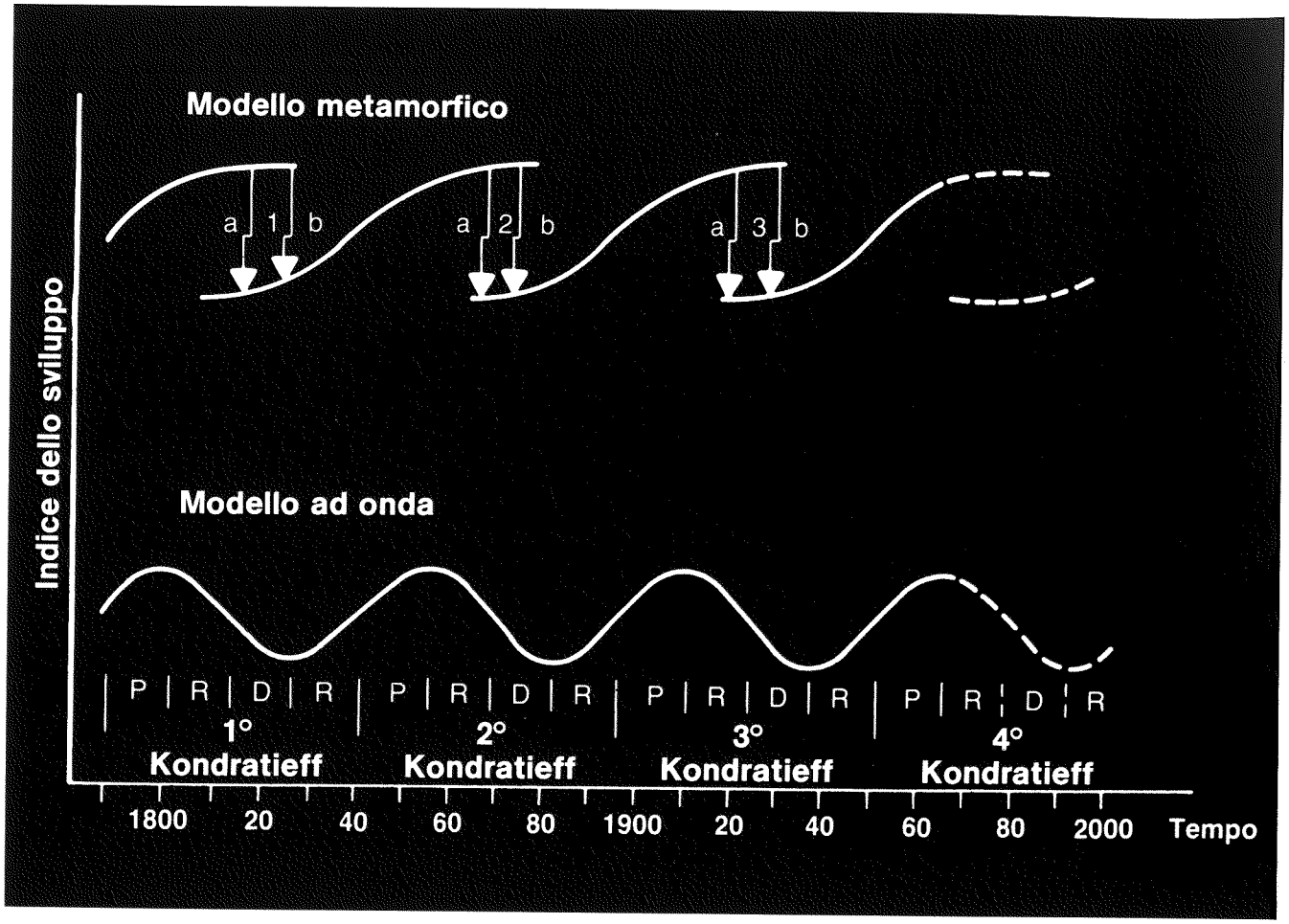


Fig. 1 - Modello metamorfico e modello ad onde.
Per Mensh (modello metamorfico) l'andamento dei cicli di vita dei diversi prodotti e tecnologie è rappresentato da curve ad S che si susseguono in modo discontinuo.
L'inviluppo di queste curve costituisce il modello ad onda tipico dell'analisi "classica" di Kondratieff, Kuznets, Schumpeter.
(In figura, le sequenze P/R/D/R indicano le fasi di Prosperità, Recessione, Depressione e Ripresa di un'onda di Kondratieff).

terpretazione dei cicli Kondratieff, mettendo soprattutto l'accento sull'opposto andamento dei prezzi relativi delle materie prime (agricoltura compresa) e quelli industriali. In particolare quando i prezzi agricoli aumentano relativamente a quelli industriali - e si ha un aumento complessivo del livello dei prezzi - si ha un periodo di crescita economica, e viceversa. Quindi, secondo Rostow, nel periodo del dopoguerra - a partire dal '55 al '72 - saremmo vissuti in un periodo di "crisi", mentre dal 1973 - con lo shock petrolifero e delle materie prime - si sarebbe entrati in un periodo di ciclo ascendente.
Su questa base, recentemente, G. Modelsky ha cercato correlazioni tra fasi del ciclo di Kondratieff e quelle della politica mondiale [18], con risultati che sono, però, molto discutibili.

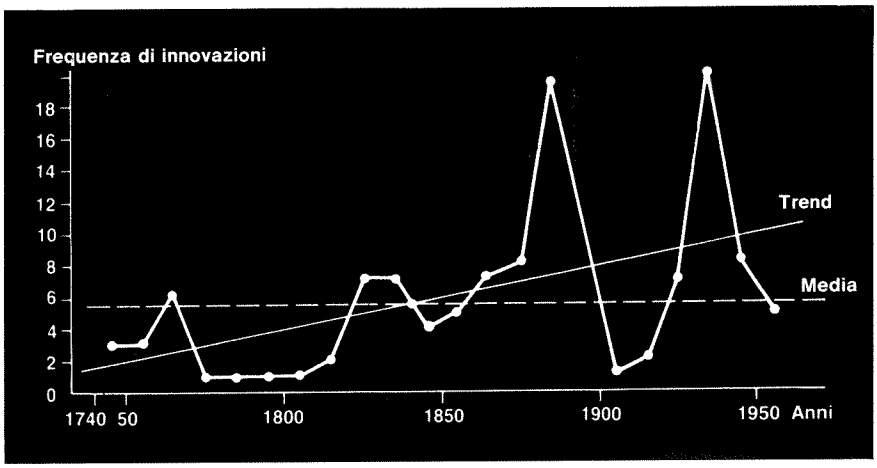
Ma è sul rapporto ciclo-innovazione che, in anni più recenti si è focalizzato il dibattito, grazie al lavoro di un economista tedesco, G. Mensh. Questi riprende grosso modo la teoria schumpeteriana dell'imprenditorialità collegandola all'apparire, nelle fasi di depressione, sul mercato di un "cluster" di prodotti innovativi. Questi prodotti creano nuovi mercati in rapida espansione (mentre quelli tradizionali sono in declino o stagnazione), nuove occasioni di profitto, favoriscono l'emergere di una innovazione nel processo produttivo anche in settori tradizionali stimolando gli "spiriti animali" degli imprenditori. L'attivazione di nuovi mercati, infine, fà uscire il ciclo economico dalla fase del declino per spingerlo verso una nuova crescita.

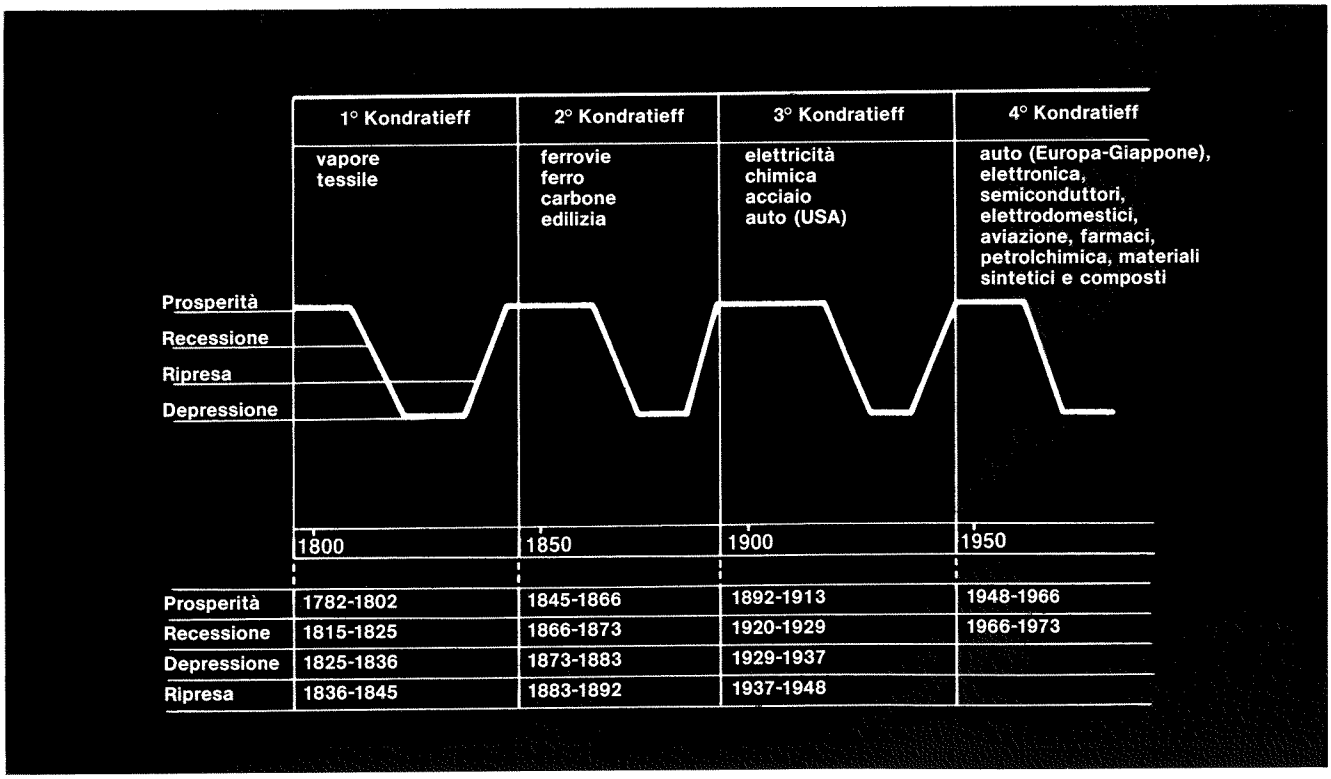
Mensh ha chiamato la sua teoria "metamorfosi", contrapposta a quella classica kondratieffiana-schumpeteriana: la curva di Mensh, in effetti, non è un'onda, ma una molteplicità di curve ad S che caratterizzano la vita marketing di un prodotto: introduzione, crescita esponenziale, maturità, declino. Nella fase di declino generale dell'attività economica si tendono a "recuperare" invenzioni magari dimenticate e, comunque, ad accelerare l'attività innovativa proprio per sfuggire alla svalorizzazione dello stock di capitale e di prodotti. Mensh ha individuato tre "cluster" di innovazioni, tre periodi nei quali, i nuovo prodotti sono apparsi sul mercato "a grappolo": nel 1825, nel 1886 e nel 1935 il numero relativo di innovazioni e la velocità stessa con cui l'innovazione si è affermata sul mercato, mostrano un picco (fig. 1 e 2).

Tab. 1 - Cicli economici e innovazione tecnologica (Van Dujin)

Tipo di innovazione \ Fase del ciclo	Depressione	Ripresa	Prosperità	Recessione
PRODOTTO (nuove industrie)	+	+++	++	+
PRODOTTO (vecchie industrie)	+++	+++	+	+
PROCESSO (vecchie industrie)	+++	+	++	++
PROCESSO (industrie di base)	+	++	+++	++

Fig. 2 - Frequenza di innovazioni di base (Fonte: Mensh).





	1° Kondratieff	2° Kondratieff	3° Kondratieff	4° Kondratieff
Prosperità	1782-1802	1845-1866	1892-1913	1948-1966
Recessione	1815-1825	1866-1873	1920-1929	1966-1973
Depressione	1825-1836	1873-1883	1929-1937	
Ripresa	1836-1845	1883-1892	1937-1948	

Fig. 3 - Schema delle quattro onde Kondratieff con l'elenco delle principali produzioni innovative (Fonte : Van Dujin).
L'andamento ad onda non rappresenta la reale dinamica delle variabili economiche (prezzi, produzione ecc.), quanto una formalizzazione che pone unicamente in evidenza l'alternarsi delle varie fasi che costituiscono l'onda "reale". Bisogna riferirsi alla fig. 4 per il reale andamento mondiale dei prezzi e della produzione.

Van Dujin ha schematizzato efficacemente l'andamento del rapporto fra innovazione tecnologica (di prodotto e di processo) con le varie fasi del ciclo (v. fig. 3 e tab. 1).

Lo stesso autore ha offerto uno schema cronologico nel quale, crediamo coerentemente, è sintetizzata l'evoluzione del sistema sociale occidentale durante le quattro onde Kondratieff che fin'ora l'hanno caratterizzato. Sulla base di questo schema, abbiamo inserito tanto i tassi di sviluppo economico per i singoli sottoperiodi, che i principali elementi di innovazione tecnico-economica caratteristici (v. fig. 4 e tab. 3).

La crescita economica è calcolata con il tasso medio annuo di sviluppo per il Regno Unito nel 1° Ciclo, e come media non pesata dei tassi di aumento medio annuo per Inghilterra, Francia, Germania e Stati Uniti per gli altri periodi.

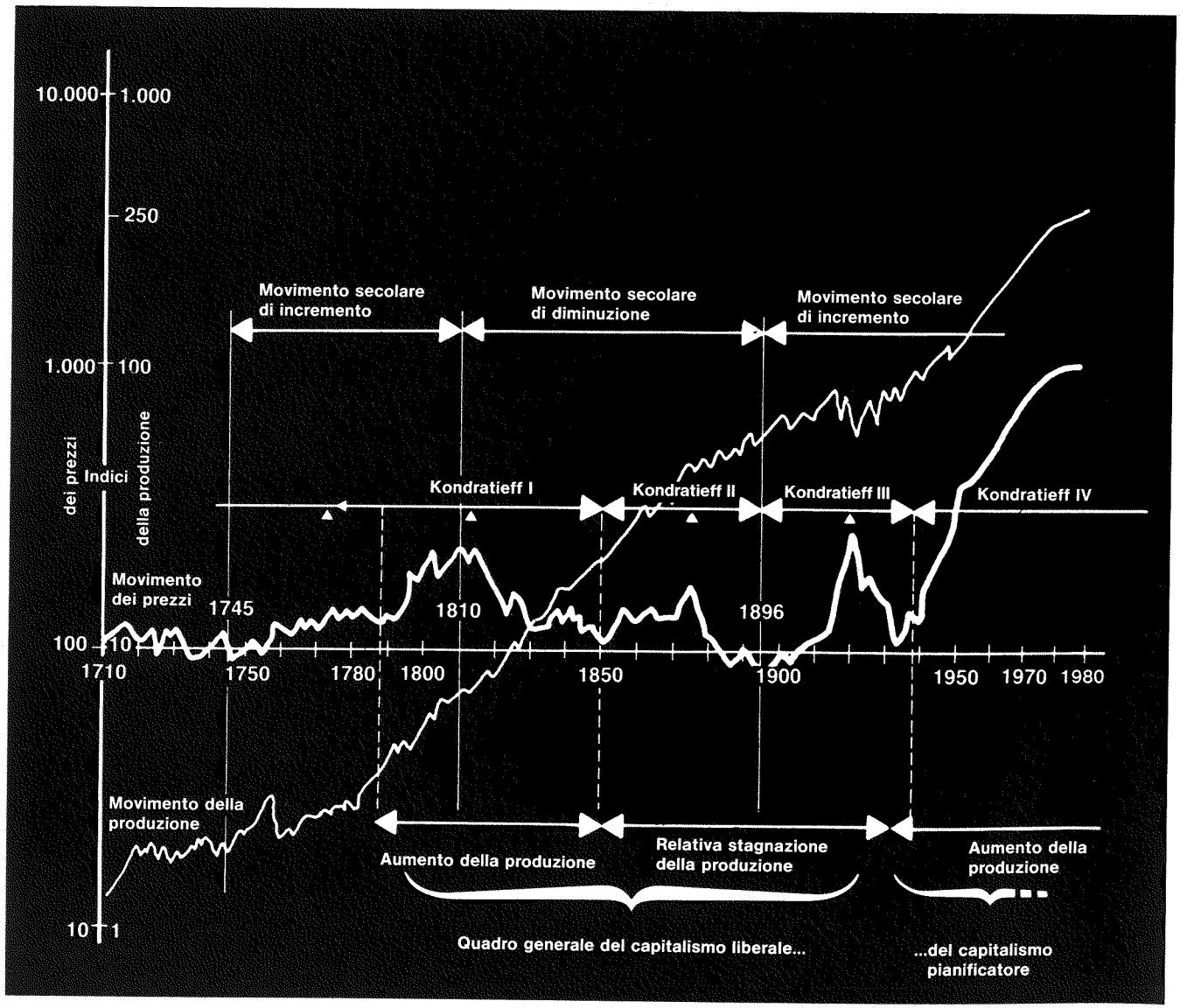
Si noti che:

a) nel primo Kondratieff non rileviamo un andamento ad onda dell'indice della produzione industriale inglese; dal punto di vista della crescita fisica, non esiste recessione e depressione; dopo le guerre napoleoniche, però, la ciclicità risulta evidente se si osserva l'andamento dei prezzi e quello del costo del denaro (vedi Kondratieff in van Dujin, pag. 74 e 78);

b) a livello disaggregato, Imbert ha

Fig. 4 - Le onde lunghe dei prezzi e della produzione mondiale (Fonte: elaborazione su Lesourd-Gèrard).

Abbiamo aggiornato fino agli anni '80 il grafico che illustra sinteticamente l'andamento plurisecolare dei prezzi e del volume della produzione per la Gran Bretagna. L'andamento ad onde della curva dei prezzi è evidente. La curva della produzione, invece, è in salita, ma l'andamento ad onda risulta percettibile nei singoli periodi qualora si passi dai valori assoluti alle variazioni della dinamica di crescita.



Tab. 2 - Evoluzione del sistema economico occidentale. Le suddivisioni orizzontali corrispondono alle quattro onde di Kondratieff.
(La produzione industriale è indicata col tasso medio annuale di sviluppo in termini reali).

Onda	Fase	Periodo	Produzione industriale	Innovazione
I	PROSPERITÀ	1782-1815	3.1	Meccanizzazione filatura e tessitura del cotone
	RECESSIONE	1815-1825	3.9	Diffusione macchina a vapore nell'industria tessile
	DEPRESSIONE	1825-1836	3.7	Ferrovie in Inghilterra
	RIPRESA	1846-1845	3.3	Ferrovie in Europa
II	PROSPERITÀ	1845-1866	3.8	Acciaio (diverse tecnologie)
	RECESSIONE	1866-1872		Chimica inorganica
	DEPRESSIONE	1872-1883	2.6	Elettricità
	RIPRESA	1883-1892		Motore a combustione interna
III	PROSPERITÀ	1892-1920	3.8	Automobili, energia elettrica telefono, meccanizzazione produzione industriale (America)
	RECESSIONE	1920-1929		Radio, fibre artificiali, meccanizzazione produzione industriale (Europa)
	DEPRESSIONE	1929-1937	2.0	Aviazione, fibre sintetiche, TV
	RIPRESA	1937-1948		Jet, silicio, energia atomica
IV	PROSPERITÀ	1948-1966	5.8	Produzione di massa di consumo (Europa), elettronica
	RECESSIONE	1966-1973		Informatica, automazione
	DEPRESSIONE	1973-198?	2.1	Automazione industriale, nuovi materiali, servizi.
	RIPRESA	?-?		Meccatronica?, automazione domestica?

rilevato la congruenza fra le serie dei prezzi e quelle delle produzioni: su 80 serie studiate, ha trovato concordanze perfette e buone con 47 serie, e nessuna concordanza con 16 serie, mentre su 265 fasi studiate, la concordanza si è verificata per il 75% dei casi. In conclusione, tenendo conto anche del lavoro di Rostow, possiamo dire che la teoria dei cicli ha un suo fondamento materiale consolidato;

c) le innovazioni presentate nella tabella sono, ovviamente, di tipo esemplificativo, nel senso che costituiscono un campione più o meno rappresentativo delle innovazioni apparse con successo sul mercato.

3. Le curve di prodotto/mercato

Van Duijn ha riorganizzato l'analisi di Mensh sulla base della cronologia dei cicli Kondratieff, trovando la correlazione illustrata in fig. 3 e tab. 3.

Il nostro obiettivo non è quello di proporre una diversa classificazione delle innovazioni/invenzioni proposta - seppure, soprattutto per gli anni del dopoguerra, una più vasta indagine sarebbe senz'altro auspicabile - quanto piuttosto esaminare come una serie significativa di queste innovazioni abbiano segnato una fase nella storia dello sviluppo economico occidentale. In particolare, prenderemo in esame la forma che ha assunto la curva di introduzione-sviluppo-maturità di alcuni prodotti su mercati significativi: Regno Unito, Stati Uniti, Germania. Tra i prodotti abbiamo scelto quelli che, ragionevolmente, possono rappresentare tappe decisive dello sviluppo tecnologico ed economico delle economie di mercato.

In tal modo si cercherà, ove possibile, di illustrare l'andamento empirico di alcune curve a S, cercando così di quantificare la teoria della metamorfosi menshiana. Per il primo Kondratieff abbiamo utilizzato, come indicatori, il consumo del cotone filato in Inghilterra, il numero di fusi, l'andamento del numero di telai a mano e meccanici in Inghilterra e Francia, il numero di macchine a vapore installate, ed, infine, la lunghezza delle linee ferroviarie nei diversi paesi.

Per ragioni che risulteranno chiare in seguito, l'interesse è limitato nella maggior parte dei casi, alla fase di introduzione e di sviluppo del prodotto sul mercato. Purtuttavia vale la pena di osservare, nei due grafici che seguono, il tentativo di Rostow di individuare, sul lungo periodo, il ciclo economico di due paesi come l'Inghilterra e gli Stati Uniti (Rostow dà la curva per 20 paesi in totale). Possiamo identificare un'onda del cotone e del ferro - prima rivoluzione industriale - un'onda delle costruzioni ferroviarie, negli anni '40 del XIX secolo, un'onda di nuovi materiali, negli anni '70, - acciaio e acido solforico - un'onda, verso l'inizio del secolo, dell'elettricità e

Fase del ciclo	N° di innovazioni
1° KONDRATIEFF	
GUERRA (1802-1815)	3
RECESSIONE (1815-1825)	3
DEPRESSIONE (1925-1836)	4
RIPRESA (1836-1845)	6
2° KONDRATIEFF	
PROSPERITÀ (1845-1866)	15
RECESSIONE (1866-1872)	7
DEPRESSIONE (1872-1883)	9
RIPRESA (1883-1892)	15
3° KONDRATIEFF	
PROSPERITÀ (1892-1920)	29
RECESSIONE (1920-1929)	5
DEPRESSIONE (1929-1937)	18
RIPRESA (1937-1948)	20
4° KONDRATIEFF	
PROSPERITÀ (1948-1966)	23
RECESSIONE (1967-1973)	4
TOTALE	160

Tab. 3 - Correlazioni tra fase economica e numero di innovazioni importanti (Van Dujin).

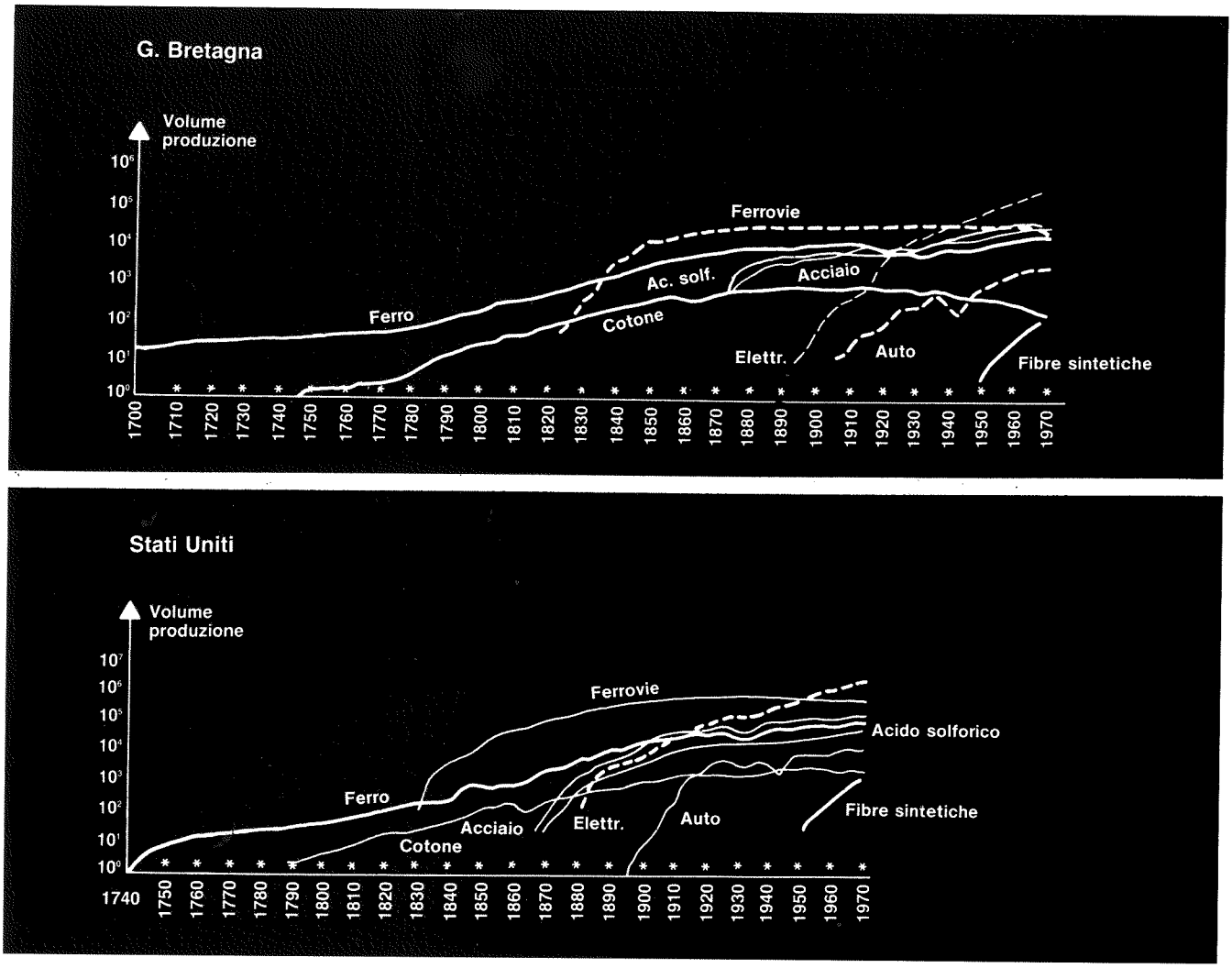


Fig. 5 - Le onde lunghe di produzioni caratteristiche (Fonte: Rostow).

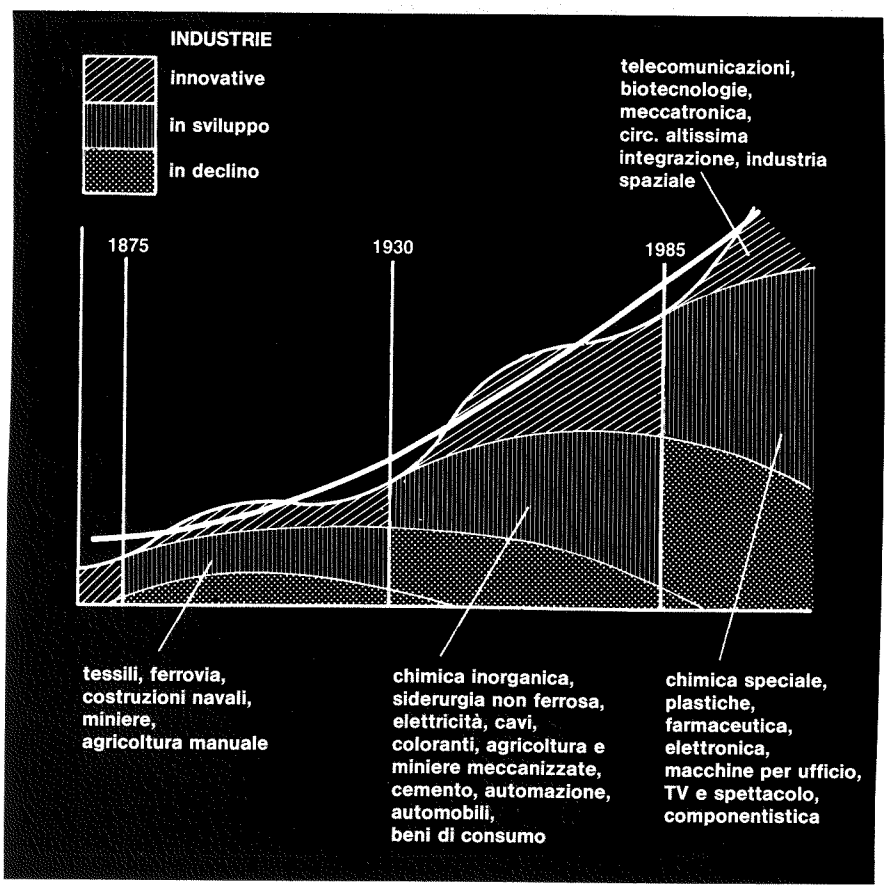


Fig. 6 - Curve inviluppo delle principali produzioni (3° e 4° periodo di Kondratieff).

dell'automobile. Storicamente alcune produzioni sono declinanti (cotone, ferrovie, ferro), altre stagnanti (automobili, acciaio), altre crescenti (elettricità, fibre sintetiche). Gruppi di queste produzioni, in ultima analisi, rappresentano bene l'andamento - e probabilmente le determinanti - del ciclo produttivo (fig. 5 e 6).

Lungi dal proporre una peculiare analisi statistica di queste serie, di seguito facciamo riferimento ad indicatori estremamente rozzi come i numeri indici e i tassi di sviluppo annuali, i quali però sono immediatamente leggibili e, per il nostro obiettivo, più che sufficienti (vedi fig. 7 per l'insieme delle curve studiate).

I° Kondratieff:

a) Crescita: Inghilterra, cotone, macchina a vapore.

1.a) Cotone. La rivoluzione industriale nasce in una delle industrie più marginali e meno avanzate dell'Inghilterra settecentesca. Tra il 1770 edil 1830 il consumo di ktm di cotone greggio passa da 1.5 a 8.2 nel 1785, a 25 nel 1800, a 56 nel 1810, a 112 nel 1830; quindi il numero indice passa da 100 a circa 7500 in 50 anni, con tasso di crescita di circa il 9% medio annuo. È interessante vedere come nel lungo periodo si sono evoluti i tassi medi di sviluppo: 3.5% annuo fra il 1750 ed il 1780; 9% fra il 1780 ed il 1810, 5.6% fra il 1810 ed il 1840: inizi lenti, accelerazione, crescita più contenuta.

1.b) Fusi. Passano da 1.7 milioni del 1780 a 4.7 del 1812, a 7 nel '19-'21, a 10 nel '29-'30, a 21 nel '50. Il tasso di crescita è stato del 3.2% nel primo periodo, del 4.5% fra il '12 ed il '29, per tornare al 3.3% fra il '30 ed il '50. È interessante notare l'andamento secolare del numero di fusi installati in Inghilterra: questi crescono a 44 milioni nel '78, a 53 nel 1908, per poi cominciare a calare a 36 nel 1938, a 9.7 nel '50, fino ad arrivare ai 2 milioni attuali: sic transit gloria mundi!

1.c) Telaio. Assieme ai fusi, il telaio è l'altro protagonista della rivo-

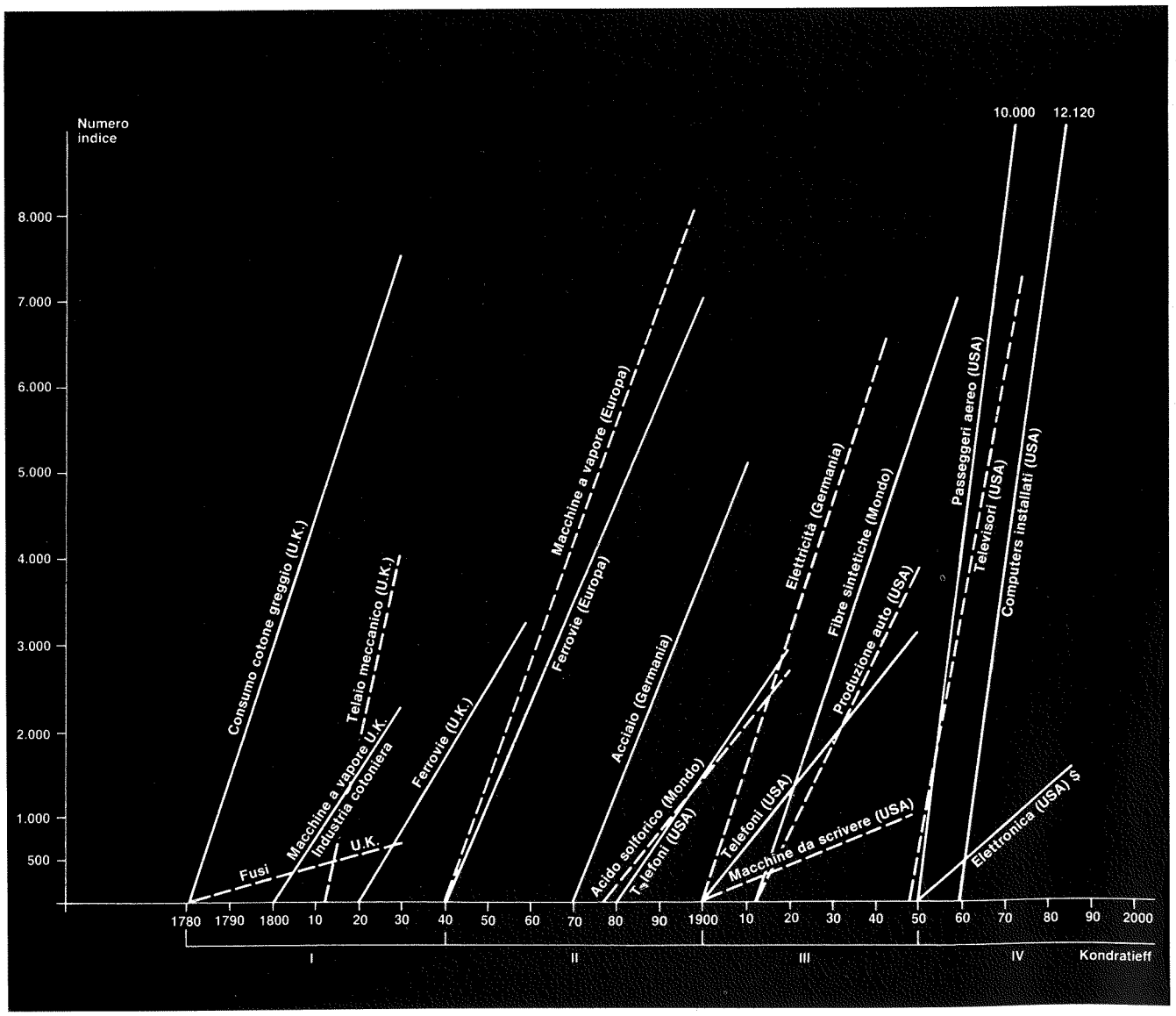
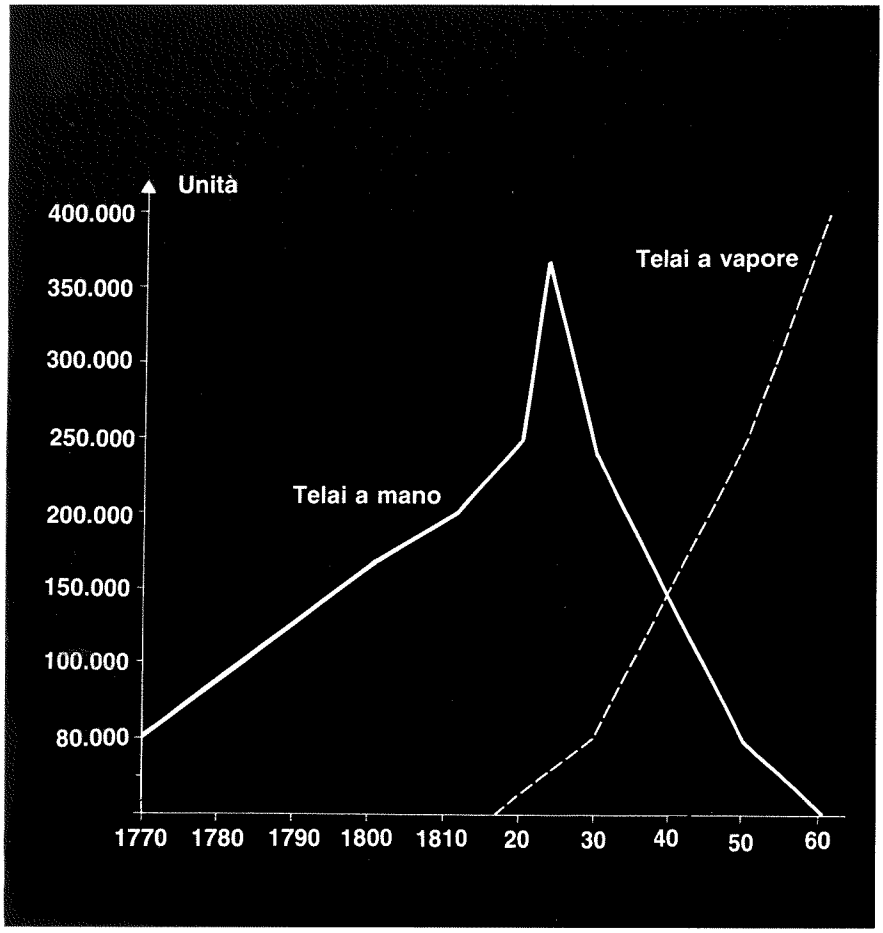


Fig. 7 - Cicli di prodotto e onde lunghe.

Fig. 8 - Gran Bretagna: evoluzione della tecnologia della tessitura.



luzione industriale. Qui possiamo vedere, con una certa chiarezza, analizzando l'andamento del parco di telai meccanici e a mano installati, l'effetto di sostituzione di una tecnologia con l'altra. La meccanizzazione della filatura provoca un consistente aumento del numero di telai a mano: questi passano da 55.000 nel 1770 a 250.000 nel 1820; contemporaneamente nel 1813 abbiamo 2500 telai meccanici, che passano a 50.000 nel 1819; dal 1820 il numero di telai manuali comincia a diminuire, mentre quello dei telai meccanici continua ad aumentare; nel 1850 ci saranno 250.000 telai meccanici e circa 40.000 a mano; nel 1861 siamo a 400 mila contro un paio di migliaia manuali (fig. 8).

1.d) Macchine a vapore. Contrariamente a quanto comunemente si crede, il motore della rivoluzione industriale è stato l'acqua, (ossia l'energia idraulica) non il vapore. Nel 1800 ci sono, in Inghilterra, circa 500 caldaie installate per una potenza di circa 12.7 KCV; di queste 104 sono installate nell'industria cotoniera, per una potenza di 2.7 KCV; nel 1830 sempre nell'industria cotoniera, la potenza sarà salita a 60 KCV (tasso di crescita 11%); tra il '30 ed il '56 il tasso di crescita diminuirà all'1,8% annuo. Nel contempo, però, l'uso del vapore investirà tutta l'economia, non solo inglese ma mondiale, producendo, lungo la seconda metà del secolo XIX - ed entrando quindi nel 2° Kondratieff - una delle più belle curve ad S disponibile (Fig. 9).

1.e) Ferrovie. L'applicazione più "industrializzante" del vapore non fu il motore per l'industria, ma la locomotiva. La ragione della mancanza di una fase di crisi nel ciclo dell'industria inglese, il boom continuato per tutta la prima parte del XIX secolo anche quando, dopo gli anni '30, il cotone abbandona la leadership dello sviluppo, sicuramente vanno trovate nell'esplosione delle costruzioni ferroviarie, che innescano processi di esportazione di capitali e di industrializzazione (nascita dell'industria meccanica).
In Inghilterra le linee ferroviarie in esercizio passano da 190 miglia del 1820 a 1688 del 1840 (11,5% medio anno), ma considerando i Km delle linee ferroviarie in esercizio nel mondo, vediamo come negli anni '30 il tasso di sviluppo è del 60% circa, del 18 negli anni '40 dell'11 fra '50 e '60, per poi decrescere al 7,6 e 5,5 nei tre decenni successivi.

2° Kondratieff

Il ciclo della seconda metà dell'800 entra nella sua fase di prosperità spinto dalla duplice ondata di meccanizzazione dell'industria - uso generalizzato della macchina a vapore

- e delle ferrovie (vedi precedenti punti ld. e le.).

Sulla base dello schema di Mensh, rivisitato da Marchetti (1982), il secondo Kondratieff vede l'emergere di nuove tecnologie innovative che si affermano negli anni della incipiente crisi (1870 e segg.); tecnologie basate essenzialmente sul ciclo dell'acciaio e sull'inizio della chimica inorganica industriale. Dal punto di vista del problema della sostituzione delle tecnologie, il caso della nave a vapore contro la tecnologia a vela sembra particolarmente rilevante.

2.a) Acciaio. Fondamentalmente lo sviluppo delle ferrovie e la nascita della moderna industria meccanica - costruzione di macchine - aveva determinato un'esplosione nell'utilizzo del ferro; l'incipiente depressione economica della fine degli anni '60 determina un'intensificazione della ricerca di nuovi sbocchi; l'emergere di nuovi processi produttivi - come il Bessemer - provoca l'emergere e l'affermarsi della nuova industria dell'acciaio. Germania e Stati Uniti sono all'avanguardia del processo di sostituzione dell'acciaio col ferro e delle nuove applicazioni dell'acciaio nell'industria meccanica e in quella delle costruzioni (nascita del cemento armato).
Il numero indice della produzione di acciaio in Germania passa da 100 nel 1870 a 548 nel 1880, a 950 nel 1885 e a 1700 nel 1890, al culmine della crisi economica: il tasso di sviluppo ventennale è del 15% medio annuo, che scenderà al 9.5% nel ventennio successivo; negli anni del "miracolo economico" del secondo dopoguerra, il tasso medio di aumento della produzione di acciaio cadrà al 7%.

2.b) Acido fosforico. Considerato l'altro elemento base della seconda rivoluzione industriale, l'indice della produzione in Germania cresce del 13% nel

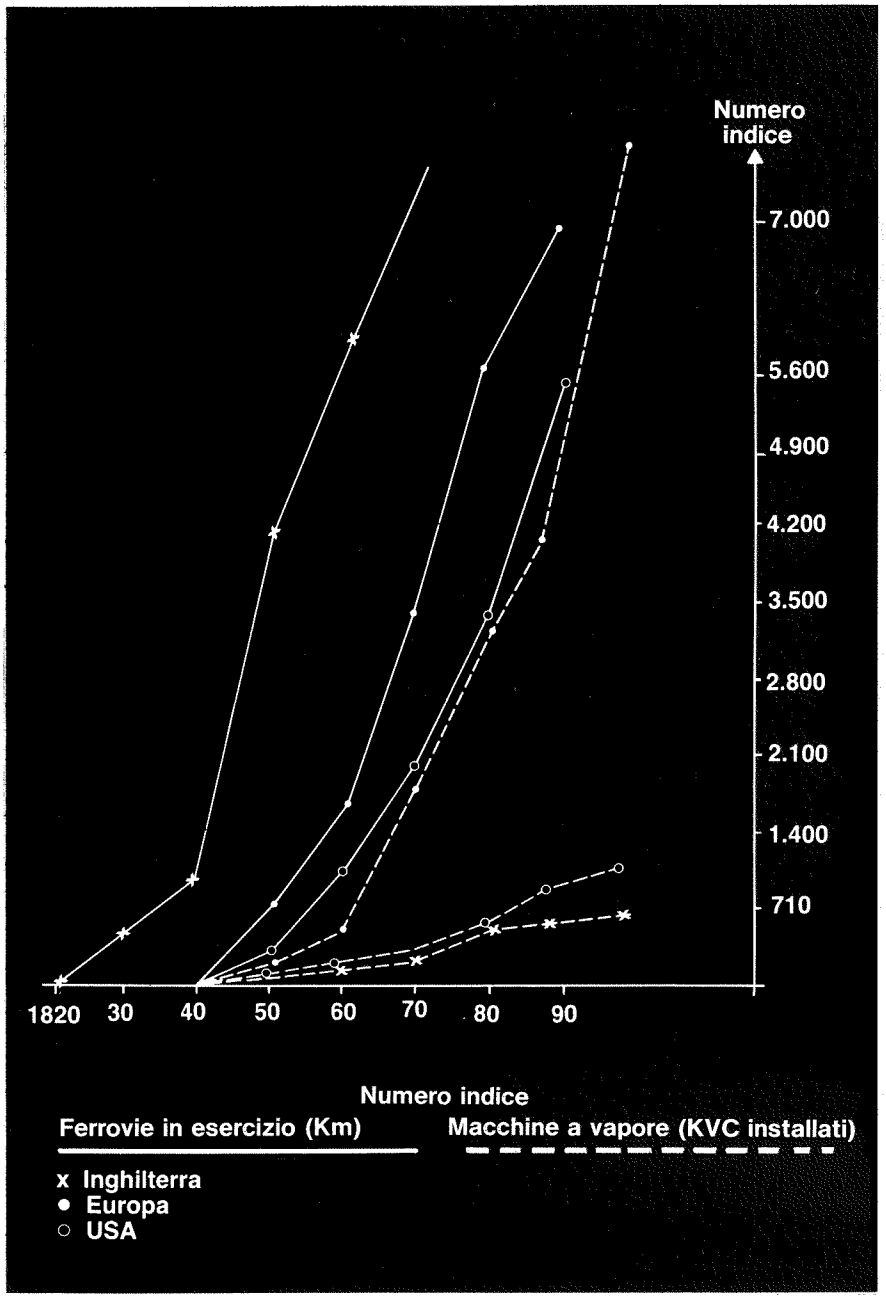
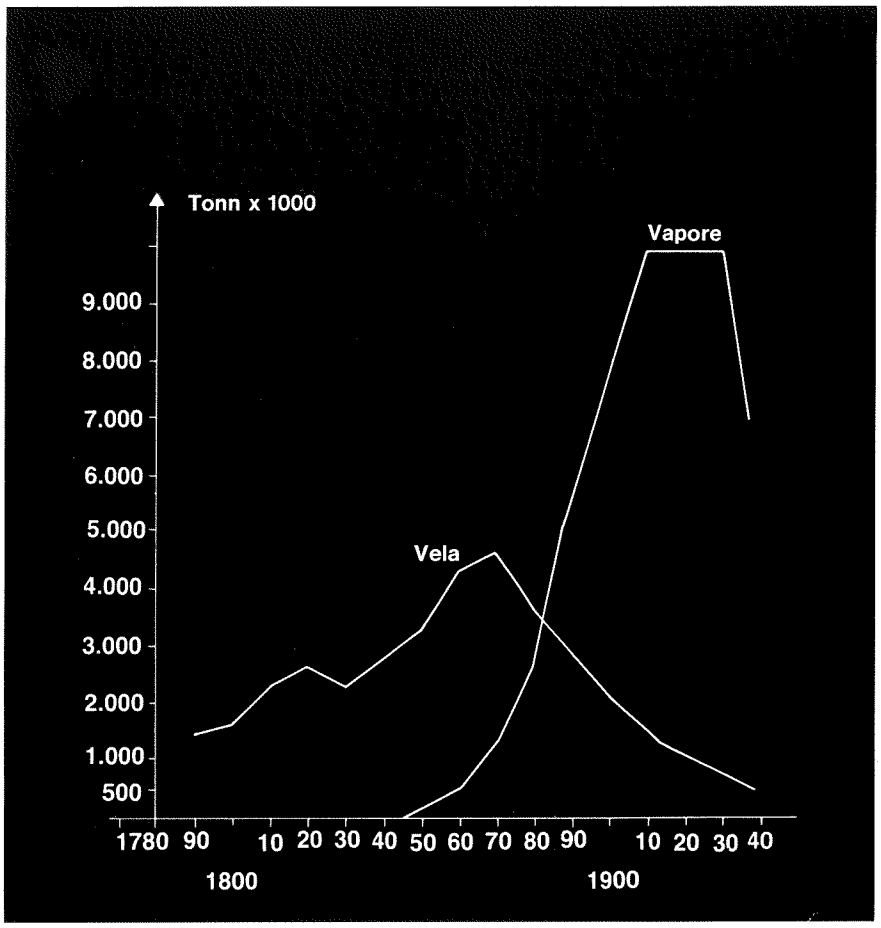


Fig. 9 - La marcia del vapore (secolo XIX).

Fig. 10 - Gran Bretagna: tonnellaggio delle navi registrate.



ventennio '70-'90 e del 6% nel ventennio successivo (e dello stesso 6% nel ventennio del miracolo del dopoguerra). A livello mondiale, fatto 100 l'indice della produzione nel 1867, questo sale a 260, nel '78, a 840 nel 1900, a 1660 nel 1913 e a 2620 nel '29: nel quarantennio il tasso di sviluppo medio è stato un pò maggiore all'8%.

2.c) Navi. Come nel caso dei telai, anche per le diverse tecnologie della navigazione le curve complessive sono estremamente esplicite: in Inghilterra il tonnellaggio delle navi a vela raddoppia fra il 1788 ed il 1815, quando appaiono le prime navi a vapore. Raddoppia ancora fra il '15 ed il '60, mentre il tonnellaggio di quelle a vapore passa da 1000 a 823 mila tonn.; a partire dal 1865 il volume della flotta a vela comincia a diminuire e nel 1885 i volumi delle due flotte si equivalgono, attorno ai 3.5 milioni di tonn. Poi mentre la crescita delle navi a vapore continua fino ai 10 milioni di tonn. del 1910, la flotta a vela si riduce, fino a diventare trascurabile negli anni '30 del nostro secolo. È interessante notare, comunque, che i 10 milioni di tonn. saranno un massimo per la flotta britannica, in quanto nel ventennio successivo non ci sarà nessun aumento; al declino dell'importanza della flotta mercantile britannica farà anche seguito la crisi della tecnologia del vapore, sostituita ormai da quella della combustione interna (fig. 10).

2.d) Seppur non possiamo considerarlo un settore "portante" dell'economia ottocentesca, conviene accennare alle origini della tecnologia telefonica, sia come una delle prime applicazioni industriali dell'energia elettrica, sia come momento dell'industrializzazione del settore delle comunicazioni, sia, infine, come preistoria di una tecnologia (telematica) che avrà un completo dispiegamento solo nel 4° Kondratieff. Il numero di telefoni in esercizio in USA passerà da 48 mila nel 1880 a 1.456 mila nel 1900, con un tasso annuo di crescita del 18%.

Il secondo Kondratieff è anche il periodo in cui alcuni paesi diventano pienamente industriali - Inghilterra, Francia, Germania, Stati Uniti - nel senso che la maggioranza della produzione e/o della forza lavoro proviene dal settore manifatturiero, mentre l'occupazione industriale si caratterizza per il rapido sorgere ed affermarsi della grande fabbrica e della moderna corporation.

3° e 4° Kondratieff

L'industria dell'auto, delle comunicazioni elettriche ed elettroniche, l'energia elettrica, l'avvento delle materie tessili artificiali e dell'aviazione commerciale, questi sono gli elementi tecnico-innovativi più significativi del periodo che ha visto l'affermazione della produzione di massa e dell'organizzazione scientifica del lavoro e dell'organizzazione industriale.

3.a) Auto. Prendendo come riferimento gli Stati Uniti, vediamo come la produzione passi da 4 mila vetture nel 1900 al 124 mila nel 1909; con l'introduzione della catena di montaggio alle officine Ford la produzione balza a 1652 mila nel 1919 facendo segnare un tasso annuo di incremento del 30% circa: il più elevato indicatore fra quelli che fin'ora abbiamo trovato assieme a quello delle costruzioni ferroviarie; tra il '19 ed il '29 il tasso di crescita cade al 10%; la produzione si dimezza durante la grande crisi e cresce del 6% medio fra il '45 ed il '69, per poi intrare in un periodo di "steady state" e di declino; nell'85 la produzione americana sarà del 20% inferiore alla punta massima del '73 (9,6 milioni di unità).

Nei paesi europei, come Gran Bretagna e Francia, avremo una partenza meno bruciante di quella americana (con sviluppi di circa il 40% inferiori a quelli americani), ma questo tasso continuerà durante la crisi (6% in media fra il '30 ed il '39 contro un misero 1% degli americani); nel dopoguerra, nella Germania del miracolo il tasso medio di crescita fino al '69 sarà tre volte quello contemporaneo americano, mentre la crescita giapponese del dopoguerra è identica a quella americana pre-1929 (Fig. 11).

Quello dell'auto, quindi, è un caso tipico di curva sensibile alla domanda e, relativamente, indifferente alla tecnologia: le curve europee e giapponesi riproducono quelle americane con circa 40 anni di ritardo.

3.b) Lo sviluppo dell'industria automobilistica indubbiamente è la causa prima dello sviluppo della moderna industria meccanica produttrice di beni di consumo; in USA l'indice di questa branca - che diventa l'asse portante dell'intera industria, passa dal 1900 al 1918 da 100 a 530, con un tasso medio

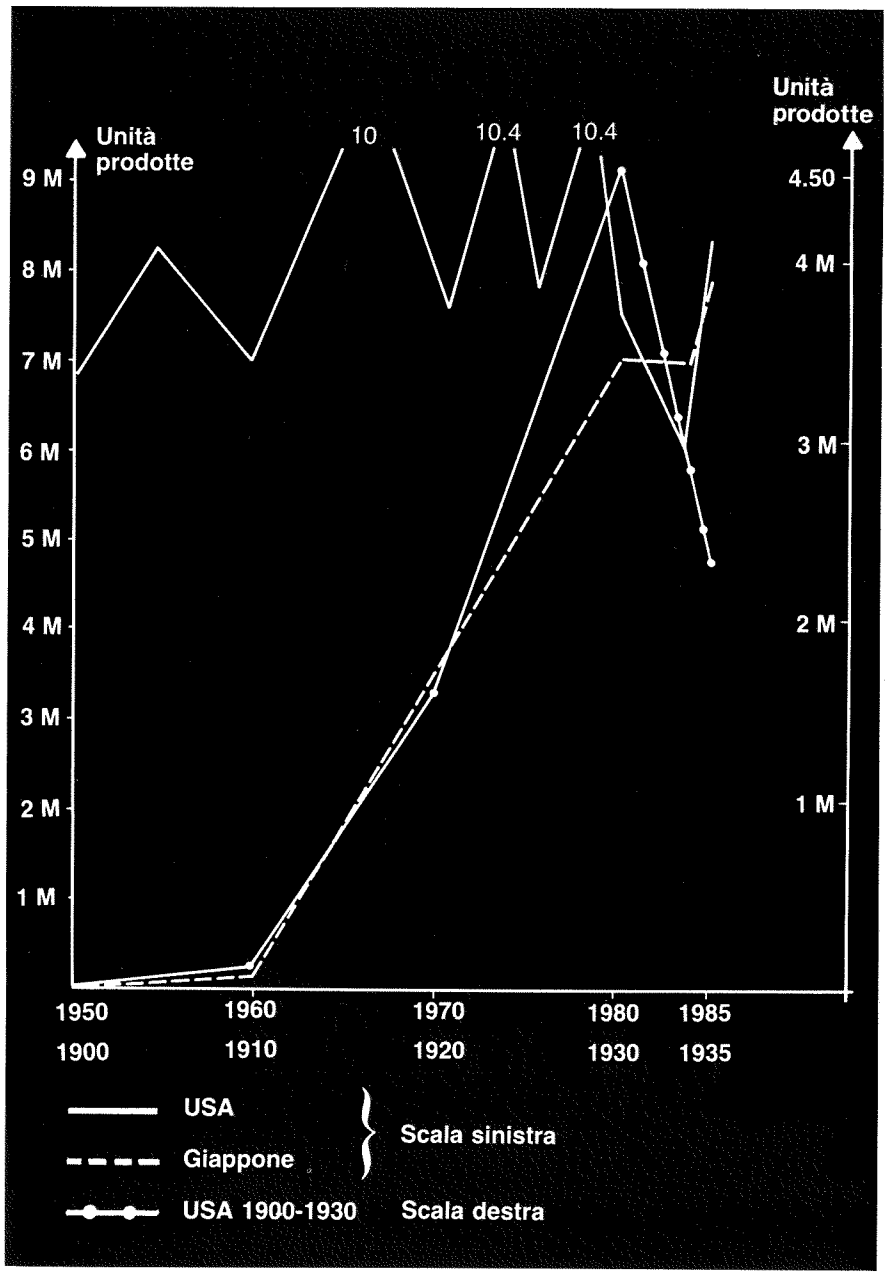


Fig. 11 - Produzione automobilistica: USA e Giappone a confronto.
La scala di sinistra si riferisce a USA e Giappone nel periodo 1950-1985, mentre quella di destra si riferisce agli USA nel periodo 1900-1935.

di sviluppo del 10%. L'industria meccanica, quindi, porta anche ad un'altro notevole cambiamento della struttura economica: il passaggio dalla meccanizzazione di fabbrica basata sul vapore a quello basato sul motore elettrico e, dunque, all'elettricità.

3.c) Possiamo vedere lo sviluppo dell'energia elettrica, tanto come crescita di una nuova branca dell'economia, quanto come esempio di sostituzione di una tecnologia - quella del vapore - con un nuova.
In Europa fra il 1900 ed il 1920 la produzione di energia elettrica cresce di 15 volte, con un tasso annuo del 14.4%, per poi assestarsi sul 7,5% nel ventennio successivo. Negli Stati Uniti la potenza fornita da motori primari a vapore raggiunge il culmine nel 1909, per poi calare regolarmente nel trentennio successivo fino a raggiungere nel '29 la metà del valore massimo; nello stesso periodo la potenza dei motori elettrici installati aumenta di 100 volte; infine si viene a creare una base di motori a combustione interna che nel periodo cresce di 10 volte. In conclusione, fra il 1899 e il 1939 abbiamo la struttura della potenza installata nei motori primari americani indicata in tab. 4.

3.d) Nuovi materiali: viscosa, rayon fibre sintetiche sostituiscono progressivamente le fibre naturali; la lunga depressione non ha nessun effetto - analogamente a quanto succede per l'energia elettrica - sulla diffusione delle nuove tecnologie che proprio in questo periodo soppiantano quelle tradizionali (Fig. 12).

3.e) Gli anni del rallentamento e della depressione ('20-'40) sono gli anni in cui nasce e si afferma - con la guerra - una nuova branca industriale: l'elettronica. Inizialmente limitata alla radio e, quindi, a materiale bellico (radar, controlli), il fatturato dell'industria elettronica americana passa dai 60 milioni di $ del '22 ai 198 M$ nel '27 ai 354 del '29 (90% in radio e valvole) per poi esplodere ai 4.5 miliardi di $ del 1944, cifra composta, per i 2/3, dalle commesse per il Pentagono. La riduzione delle spese militari del dopoguerra fa scendere il valore delle vendite di materiale elettronico a 2 miliardi di $ nel 1950, dopodiché la corsa ricomincia arrivando a 10 miliardi nel '59 (dei quali solo il 20% alle vendite di materiale radio). Il fatturato nel '75 sarà di 42 miliardi di dollari, per crescere ai 106 del 1980 e ai 150 del 1980 per poi arrivare ai 204 del 1985. Complessivamente per il ciclo dell'*elettronica* possiamo evidenziare i seguenti tassi di sviluppo:

1922-29	1929-44	1950-59
28.9%	18.6%	19.6%
1960-70	1970-80	1980-85
10.8%	16.9%	14.0%

È interessante notare come non si veda una prossima saturazione per lo sviluppo di questo complesso tecnologia-mercato, mentre, nello stesso periodo, si è avviata a saturazione tanto il mercato dell'automobile che quello dell'acciaio che avevano caratterizzato le ondate innovative precedenti.
Non solo: l'elettronica è nata principalmente come industria produttrice di beni di consumo (radio) e, soprattutto negli anni '50, l'elemento trainante dello sviluppo del mercato è stata l'introduzione e la vendita della TV a colori. Nel 1950 sempre sul mercato statunitense furono venduti 8 milioni di apparecchi radio e 7 milioni di TV bianco e nero; nel '56 le TV a colori vendute furono 100 mila, per poi balzare a 1 milione del '64. Ma a partire dall'inizio degli anni '70 l'elettronica di consumo comincia a mostrare segni di saturazione - il comparto consumer cresce solo del 180% fra il '75 e l'83 contro una crescita globale del settore del 250%, mentre struttura portante dell'elettronica diventano le macchine per l'elaborazione dei dati che nello stesso periodo triplicano le vendite (Fig. 13).

3.f) Per concludere l'analisi dei principali momenti innovativi del 4° Kondratieff conviene riferirsi ad un settore dei trasporti, nel quale la tecnologia fondata sugli aereomobili sostitui-

Tab. 4 - Potenza installata dei motori primari in USA.

	1899	1939
MACCHINA A VAPORE	79.5	9.8
TURBINA	-	17
MOTORE A COMBUSTIONE	1.3	2.7
IDRAULICA	14.5	2.4
MOTORE ELETTRICO	4.7	68.1
TOTALE	100	100
KCV	10061	66530

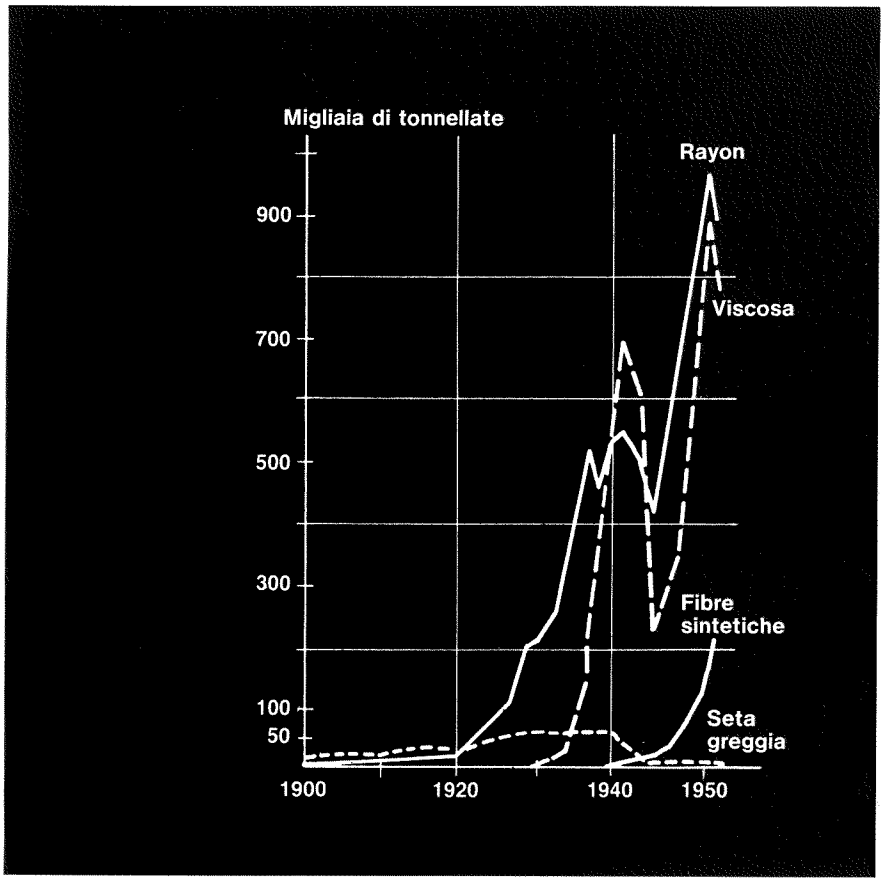


Fig. 12 - Sviluppo dei materiali tessili artificiali (1900-1950).

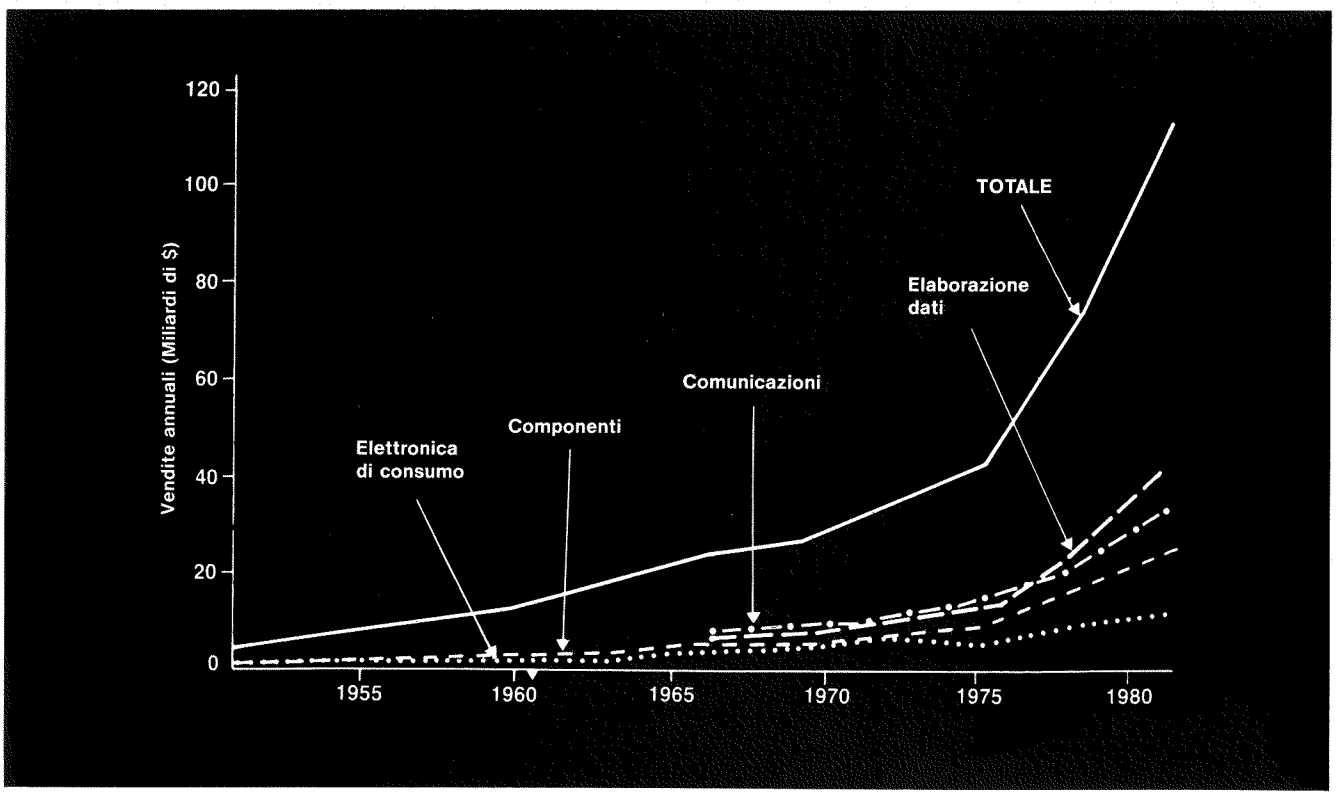


Fig. 13 - Sviluppo dell'industria elettronica statunitense.

Periodo / Scala	1956-1960	1961-1965	1966-1970	1971-1975	1976-1980
I (2,0%)	50-100 Monochrome TV sets	100-200	200-500 Color TV sets passenger cars	500-1,000	1,000-2,000
II (1.0%)	20-50 Transistor radios, nylon,	50-100 Polyester, supertankers	100-200 Tape recorders (popular model), computers	200-500	500-1,000
III (0,5%)	10-20 Washing machines, power-driven cultivators, vinyl chloride	20-50 Acryl, stereo sets, rolling mills, polyethylene, multivitamin tablets	50-100 Desk-top calculators	100-200 Nuclear power plants, rotary engine-powered cars	200-500 VTR, ICs, computers
IV (0.2%)	5-10 Transistor, electric rice cookers, synthetic rubber, miniature tubes, industrial measuring equipment, turbojets	10-20 Vinylon, vacuum cleaners, polystyrene	20-100 polypropylene, electrostatic copiers, ICs, car stereos	50-100 Microwave ovens, prefabricated housing units	100-200 Electronic watches, computer terminals
V (0.1%)	2-5 Synthetic-fiber making machines	5-10 Glass fibers	10-20 Numerically controlled machine tools, silicon rectifiers	20-50 Electronic cash registers, heavy oil desulfurization, fuel gas desulfurization, vending machines, electronic exchangers, space heaters automatic railway ticketing systems	50-100 Electronic exchanges, key telephones
VI (0.05%)	1-2 Electronic microscopes	2-5	5-10 Traffic control systems	10-20 Synthetic leather for clothing, LNG tanks, environmental pollution measuring instruments	20-50 Facsimiles, X-ray computed tomography, industrial robots, solar water heaters
VII (0.02%)	0.5-1 Transfer machines	1-2 Hydrofoils	2-5 Machining centers	5-10 Microcassette tape recorders, automated multitiered warehouses, cash dispensers	10-20 Bedclothes dryers, video games

Tab. 5 - Importanza e sviluppo dei principali settori in Giappone. I numeri romani delle ordinate rappresentano il peso, in termini di reddito nazionale, dei vari settori; i numeri arabi in ciascuna casella sono il valore della produzione, in migliaia di miliardi di Yen, per ciascun periodo.
(Fonte: M. Moritani, *Modern Industrial Technology of Japan*).

sce progressivamente quella del treno, della nave, e ora, dell'automobile. I passeggeri trasportati salgono in America dai 6 mila del 1926 al milione del 1935, ai 2,6 milioni del 1940, per esplodere ai 19 milioni del '50, ai 62 milioni del '60, ai 205 milioni del '75: il tasso medio d'aumento è stato del 22% fra '40 e '50, del 13 fra '50 e '60 e dell'8% nel quindicennio successivo.

4. Quale tecnologia sta emergendo tra 4° e 5° Kondratieff?

Cosa abbiamo evidenziato fino ad ora? Semplicemente che, in determinati periodi e per determinati prodotti - siano essi industriali o servizi - esistono dei momenti in cui lo sviluppo è particolarmente intenso, eccedendo complessivamente dalle 3 alle 10 volte il tasso di sviluppo medio dell'economia. Possiamo affermare che questi prodotti e i loro tassi di sviluppo associati determinino in qualche modo lo sviluppo dell'economia? Purtroppo, allo stadio attuale degli studi, ciò è impossibile e né Kondratieff, né Shumpeter, né Rostow o Marchetti hanno potuto stabilire un rapporto di causa fra lo sviluppo di certi settori e quello dell'intera economia. Per far ciò bisognerebbe semplicemente disporre di adeguate tavole di input/output dell'economia per i periodi in questione, ma questo, come è noto, non si ha.

Peraltro è del tutto ragionevole – anche se di impossibile dimostrazione – ritenere che la meccanizzazione dell'industria tessile nell'Inghilterra di fine'700, le costruzioni ferroviarie nel mondo negli anni '30 e '40 del XIX secolo, lo sviluppo della chimica e dell'acciaio in Germania e USA alla fine dell'800, l'industria automobilistica e dell'elettronica di consumo nel secondo dopoguerra, sono stati fenomeni che hanno caratterizzato dinamicamente la struttura produttiva ed economica dei paesi occidentali e del mondo intero.

Recentissimamente un ricercatore del MITI, M. Moritani, ha studiato l'impatto economico delle ondate successive di innovazione sul mercato giapponese dal '56 ad oggi, misurando, contemporaneamente, il peso in termini di valore aggiunto industriale dei singoli sottosettori. I risultati sono espressi nella tab. 5: come ci attendevamo, i settori più dinamici – e, al contempo quelli con maggior peso economico – sono stati, fino agli anni '70, quelli produttori di beni di consumo elettronici e dell'auto. A partire dagli anni '70 la leadership in termini di sviluppo è stata assicurata dai nuovi segmenti dei calcolatori elettronici (classe II), dei circuiti integrati e dei videoregistratori (classe III), dei robot (classe VI) e di altri materiali basati sulla micro elettronica. Sulla base poi di una minutissima analisi basata sui prodotti, l'autore ha costruito un modello previsionale evidenziando i prodotti innovativi per il quindicennio 1985-2000. I risultati, in termini di prodotto, sono riportati nella tabella 6 e, come si vede, per l'essenziale si tratta di prodotti legati all'elaborazione automatica dell'informazione e alle tecnologie ad essa relative, ad esempio fra i nuovi materiali la ceramica ed il silicio.

Dal punto di vista dei valori assoluti, abbiamo schematizzato nella tabella 7 la situazione fino al 2000.

Sotto la voce "altro" sono comprese le biotecnologie, l'energia, l'industria spaziale; inoltre il tasso di sviluppo globale dell'economia per il quindicennio è stimato nel 4.7% medio annuo.

La situazione, quindi, sembra piuttosto chiara: l'elaborazione automatica dell'informazione non solo sarà la locomotiva dello sviluppo giapponese fino al 2000, ma il peso di questa sull'economia complessiva passerà dall'attuale 7% a circa un quarto del valore aggiunto.

Scala \ Periodo	1980-85	1985-90	1990-95
I			
II	VTRs	ICs	ICs
III	ICs	Video camera-recorders	High-definition TV sets
IV	General-purpose computers, external memory, numerically controlled machine tools	Video disks, semiconductor-production equipment, personal computers	Comprehensive information terminals for home, work stations, digital networks, combined cycle generation
V	Office and personal computers, semiconductor-production equipment, VTR tapes, lead frames, industrial robots	Word processors, CAD/CAM, minicopiers, facsimiles, page printers, optical disk memory, optical communications systems, compact disk software, video disk software, ceramic sensors.	Expert systems, color printers, electronic cameras, mobile phones, CATV, ceramic engine parts, separation membrane, intelligent robots, genetically engineered pharmaceuticals
VI	Printers, facsimiles, key telephones, video cameras, ceramic packages for ICs, silicon wafers	Disk materials, electromagnetic wave shielding materials, pocket-size TV sets	Gallium arsenide ICs, solar batteries amorphous metals, fuel cells, heat pipes, laser metal-working equipment
VII	Computerized citizen-band radio, carbon fiber	Supercomputers, computerized tomography laser scalpel, laser metal-working equipment, carbon fiber	Shape-memory alloys, superconductive materials, aircraft jet engines

Tab. 6 - Sviluppo atteso e peso di alcune produzioni in Giappone (vedi tabella precedente per la fonte ed il significato delle scale).

	1985	1990	1995	2000	1985/2000 (*)
ELETTRONICA/INFORMATICA	18	32	57	100	12.1
NUOVI MATERIALI	2	3	5	8	9.7
ALTRO	1	2	4	10	16.6
TOTALE	21	37	66	118	12.2
% PRODUZIONE INDUSTRIALE	8.8	12.8	19	27.9	

Tab. 7 - Mercati ad elevata tecnologia. Le cifre sono in migliaia di miliardi di Yen. L'ultima colonna (*) si riferisce all'incremento percentuale annuo medio.

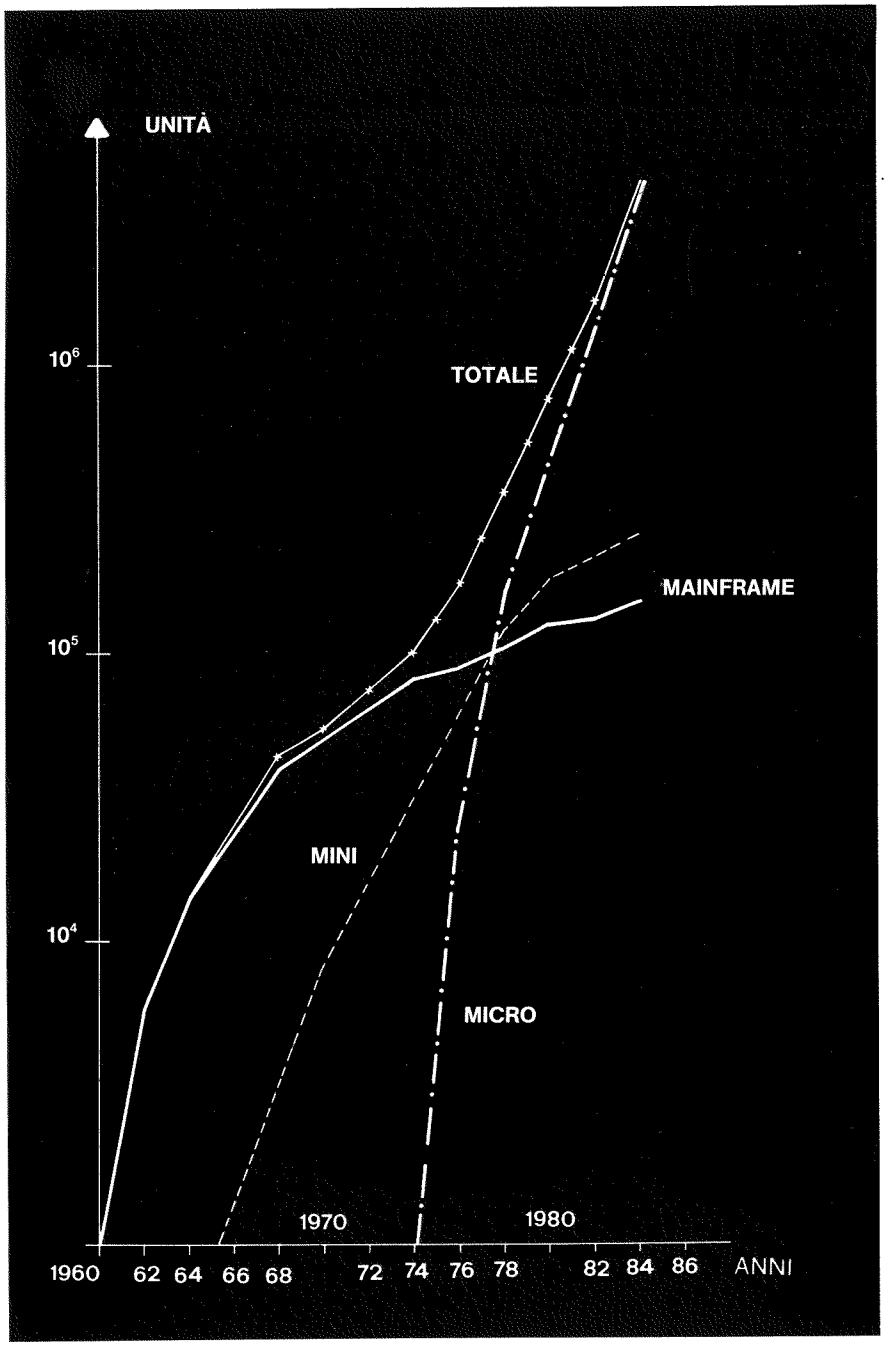


Fig. 14 - USA: parco installato di elaboratori elettronici (in unità). Gli elaboratori sono suddivisi per classe di prezzo: micro da 1 a 2 K$, mini da 2 a 25 K$, mainframe: oltre 25 K$. (Fonte: Bureau of Economic Analysis).

Facciamo ora un passo indietro, tornando all'industria americana negli anni'60. Come abbiamo visto, è in questo periodo che l'industria dell'informatica comincia a crescere a un ritmo sensibilmente superiore a quello medio del comparto e il settore si configura in una fase di transizione fra l'elettronica di consumo e quella dei beni industriali.

Questa fase si accentua nel momento in cui la crescita dell'intera economia, a partire dalla metà degli anni '70, comincia a declinare ed arrestarsi. Quindi, coerentemente alla tesi di Mensh, è in periodo di recessione e di crisi che un nuovo settore emerge e si afferma, sviluppando caratteristiche fortemente innovative. Le curve di crescita, per gli USA, del parco elaboratori installati, della spesa per hardware e di quella per software sono estremamente significative, anche se confrontate con quelle date per i prodotti che hanno caratterizzato i precedenti cicli innovativi. L'elaboratore elettronico si è caratterizzato nel passato venticinquennio come un bene di produzione che si è venduto come un bene di consumo durevole; solo l'industria americana dell'auto, ai suoi inizi, ha mostrato, per un breve periodo, tassi di sviluppo superiori.

Si consideri, inoltre, che se nel '60 il peso delle macchine per elaborazione dei dati sull'investimento totale in macchinario era del solo 2,8%, nel 1985 siamo giunti al 21%; e questo non solo negli Stati Uniti: in Italia, sempre nel 1985 il rapporto era superiore al 16%.

Ma non è forse lo stesso peso acquisito all'interno dell'economia del settore dell'elaborazione dei dati che fá pensare - assieme alla ormai biennale stasi del mercato americano - ad una sorta di saturazione del mercato? Saturazione che, certo, non si esprime come nel passato decennio per i settori dell'auto e

dell'acciaio in una stagnazione o recessione della produzione, ma, piuttosto, in un tasso di sviluppo ad una cifra, piuttostoché a due cifre come è stato nello scorso decennio.

Limitiamoci al momento all'analisi dell'hardware tralasciando il software al quale gli analisti economici continuano a garantire nel prossimo quindicennio uno sviluppo a due cifre. Esaminiamo in dettaglio le curve delle installazioni americane per tipologia di prodotto, dal 1960 ad oggi, distinguendo fra mainframe, mini e micro (fig. 14 e 15).

Appare evidente il succedersi di tre ondate di sviluppo - che configurano tre veri e propri mercati - che sono conseguenti a tre famiglie di innovazione tecnologica: quella dei mainframe, quella dei mini e quella dei micro.

Ciò che è rilevante è non solo la sostanziale uniformità di altri mercati nazionali a quello americano - basti vedere la curva per l'Italia a pag. 63 di "Italia Informatica" [23] - ma il fatto che ciascun mercato non sostituisce il precedente ma si somma a quello: la curva inviluppo è quindi costantemente in salita.

È probabile che tale modello di sviluppo continui nel prossimo quindicennio: ad uno sviluppo consistente, ma ridotto, di quella che ormai possiamo chiamare l'informatica "classica", si somma lo sviluppo impetuoso di nuove applicazioni che, nei prossimi anni, faranno segnare tassi di sviluppo superiori al 20%. Prima di accennare ai principali settori espansivi, varrà la pena di ricordare come le previsioni elaborate dal BEA e dal CBMA per il mercato americano – da qui al '95, un tasso medio di sviluppo dell'hardware del 8.7% - pongono pur sempre l'industria dell'elaborazione automatica dei dati ad un tasso di sviluppo che è circa tre volte quello medio dell'industria americana.

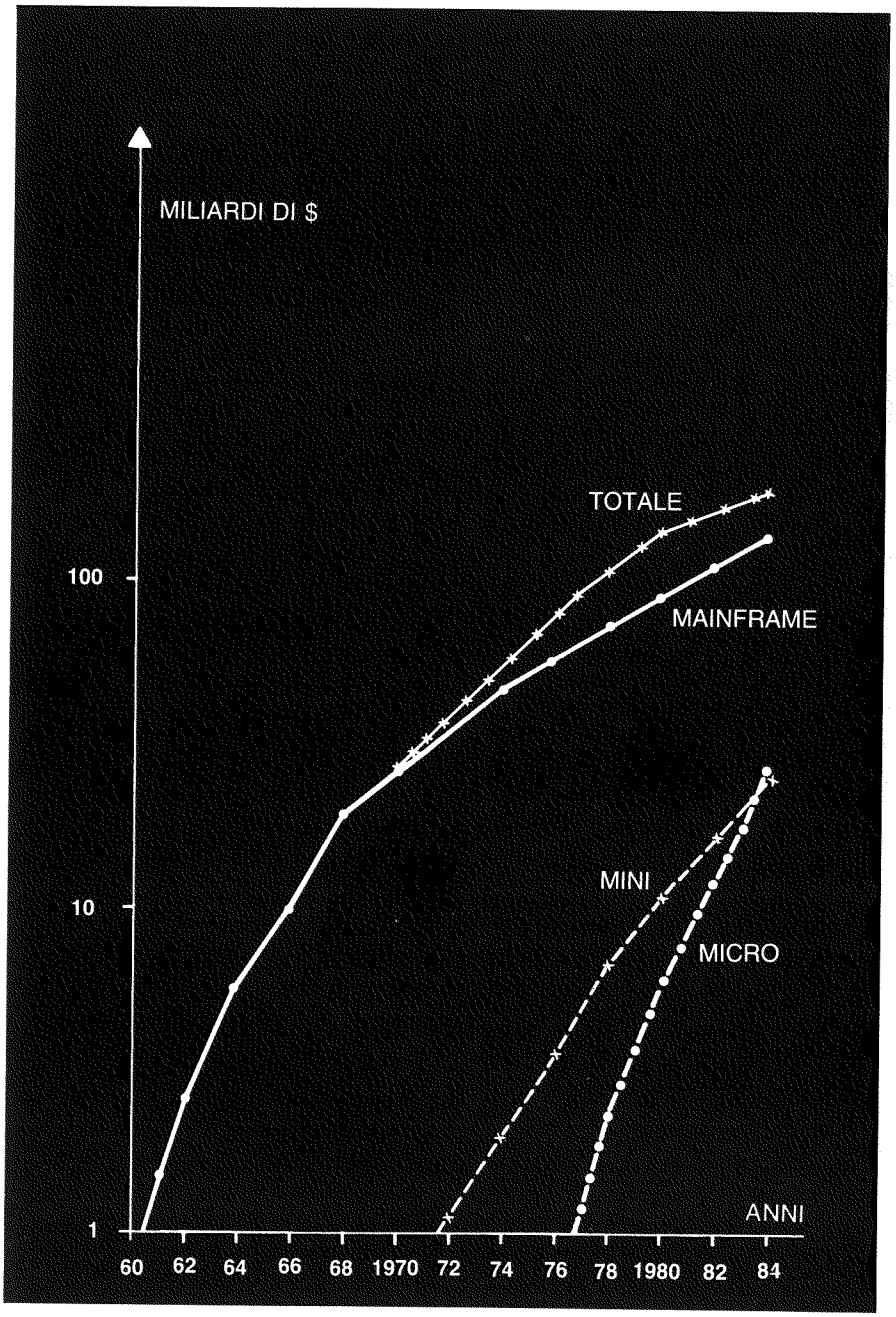
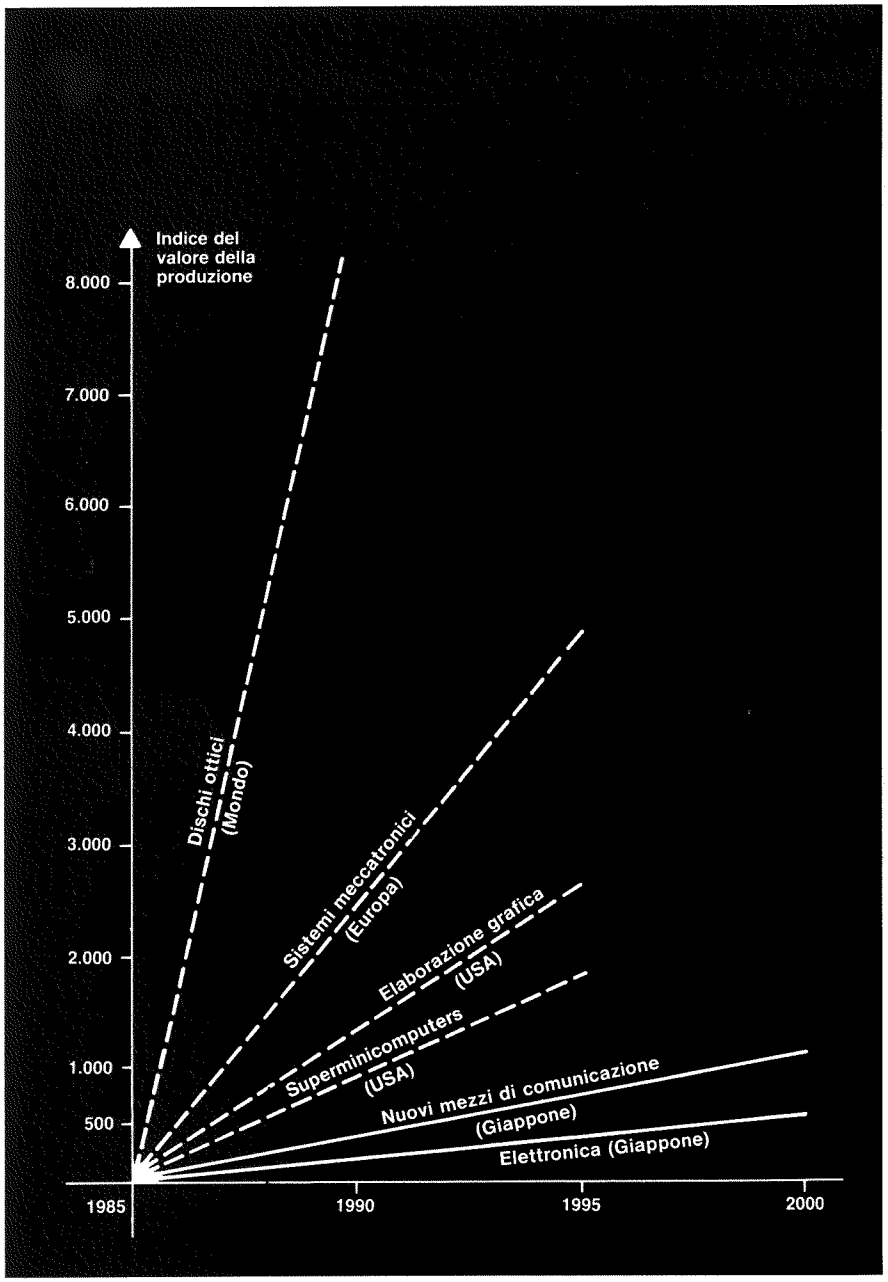


Fig. 15 - USA: parco installato di elaboratori elettronici (in valore). (Fonte: Bureau of Economic Analysis).

Fig. 16 - Tassi di sviluppo attesi per alcune produzioni del settore informatico.



Tab. 8 - Settori di mercato informatico con più elevato tasso di innovazione (B$ = Miliardi di dollari).

Mercati	Valore di mercato mondiale 1991 (B$)	Crescita % annua (1986-91)
MINISUPERCOMPUTER	1.76	34
STAZIONI LAVORO TECNICO/SCIENTIFICHE	4.43	30
PROCESSORI SIMBOLICI	4.0	50
GRAFICA GESTIONALE E SCIENTIFICA	35.0	37
DISCHI OTTICI	8.7	150
ELABORAZIONE DELLA VISIONE	.5	35
SISTEMI ESPERTI	1.4	65
CHIP ARSENIURO-GALLIO	4.2	59

	Fabbrica	Ufficio	Casa	Comunicazione	Totale
1983	4.8	8.6	--	--	13.4
1990	9.6	27.0	2.9	3.3	42.8
1995	18.3	58.9	7.4	7.5	92.1
83/90%	10.4	17.8			15.5
90/95%	13.7	16.9	20.7	18.0	16.6

Tab. 9 - La domanda di prodotti informatici suddivisa in quattro aree di utenti finali, nel periodo 1983-95 (Fonte: MITI).

A questa situazione - comunque estremamente dinamica - si somma poi, lo sviluppo dei singoli sottosettori innovativi che faranno segnare ritmi di sviluppo senz'altro notevoli.

All'interno di questi settori ad elevata dinamica, abbiamo selezionato alcuni che appaiono strategici come regolatori del futuro sviluppo non solo dell'elaborazione automatica dell'informazione, ma del complesso dell'economia; settori che, in altre parole, sono destinati a giocare il ruolo di industrie industrializzanti per l'intero comparto.

I settori presi in considerazione sono, inoltre, quelli più innovativi nei quali, però, l'innovazione è uscita dallo stadio sperimentale ed è già consolidata in prodotti presenti sul mercato.

Questi mercati, lungi comunque dall'esaurire anche in parte la gamma dei settori ad elevato tasso di crescita, sono quelli di fig. 16 e tab. 8, con l'annesso tasso annuale di crescita nel periodo 1986-91.

Siamo di fronte ad una tecnologia allo stato nascente - quella legata all'optoelettronica - a tecnologie in via di sviluppo - legate all'elaborazione dei simboli, delle immagini e dei linguaggi naturali o "quasi" naturali - a tecnologie più assestate e avviate alla produzione di massa - elaborazione grafica legata all'ambiente scientifico e commerciale. Nel complesso questi settori sono destinati a trainare il mercato informatico nel prossimo quinquennio, quando, per l'insieme del settore, il tasso di sviluppo previsto a livello mondiale è attorno al 13-16% annuo.

In altre parole, la tecnologia dell'elaborazione automatica delle informazioni sta passando dall'intervento su una specifica fonte di informazione - i dati - ad un'altra, basata sulle immagini e i simboli, mentre egualmente importante si profila l'elaborazione automatica della terza fonte di informazione, la voce.

È interessante, per concludere, rifarci ancora una volta ad uno studio del MITI volto a verificare la domanda di prodotti informatici nel prossimo quindicennio, suddividendo la domanda secondo quattro grandi tipologie di utenti finali: la fabbrica, l'ufficio, la casa e i nuovi mezzi di comunicazione. La stima fatta, prendendo come base il 1983, per i vari mercati è quella di tab. 9.

Si sconta quindi, un'accelerarsi del trend di sviluppo dopo il 1990 per l'informatizzazione massiccia di settori dell'economia finora rimasti esclusi, quali l'abitazione - e quindi l'addomesticamento dell'informatica - e nuovi mezzi di comunicazione di massa (videotex, TV via cavo, TV ad elevata definizione, ecc.).

Se questo avverrà, è abbastanza probabile che verso il '90 dovremo entrare nella fase espansiva che segna la transizione fra il 4° ed il 5° Kondratieff, riaprendo il ciclo di un venticinquennio di sviluppo e prosperità.

5. Bibliografia

[1] Berg, A. *The Age of Manufactures,* Fontana, 1986.

[2] Berg, A. *La questione delle macchine,* Il Mulino, 1981.

[3] Duijn, J.J., van *Long Waves in World Economy,* Allen & Unwin, 1983.

[4] Dupriez, L.H. *Des Mouvements economiques generaux,* Droz, 1955.

[5] Forrester, J.W. *Growth Cycles,* in De Economist, (Amsterdam), 1977.

[6] Forrester, J.W. *Innovation and Economic Change,* in Futures, 1981.

[7] Freeman, C. (ed.) *Long Waves in World Economy,* Butterworths, 1983.

[8] Imbert, G. *Des mouvements de long dureé Kondratieff,* La penseé universitaire, 1960.

[9] Kondratieff, N. *I cicli maggiori,* Cappelli, 1983.

[10] Kuznets, S. *Secular Movements in Production and Prices,* Boston 1930.

[11] Lesoud J.A., Girard C. *Storia economica dell'800 e del '900,* ISEDI 1974.

[12] Maddison, A. *Phases of Capitalist Development,* OUP, 1982.

[13] Mandel, E. *Long Waves of Capitalistic Development,* CUP, 1980.

[14] Marchetti, C. *Innovazione, industria, economia. Una analisi di inviluppo,* in G. Antonelli (ed): Innovazioni tecnologiche e strutture produttive. Il caso dell'Italia. Il Mulino, 1984.

[15] Marchetti, C. *Invention et innovations: les cycles revisités,* in Futuribles, Mars 1982.

[16] Mensh, G. *The Technological Stalemate,* Ballinger, 1979.

[17] MITI *The Future of the Japanese Electronic Industries,* Tokio 1986.

[18] Modelsky, G. *On the Interdipendence of Political and Economic Fluctuations,* in Economie Appliqueé, 1982.

[19] Riview no. 4, anno VII, 1984. Numero dedicato ai cicli.

[20] Rosier, B., Dockes, P. *Rytmes Economiques,* Maspero, 1983.

[21] Rostow, W.W. *The World Economy,* Texas U.P., 1978.

[22] Schumpeter, J. *Business Cycles,* Mc Graw Hill, 1939

[23] AAVV *Italia informatica,* Ediz. Sole/24 Ore, 1986

Il lavoro qui presentato è consistito essenzialmente nell'individuare serie coerenti di statistiche riguardanti i prodotti considerati. I volumi di Mitchell sulle statistiche storiche europee, americane e giapponesi (Macmillan, 1978 e segg.) ci hanno fornito l'essenziale delle serie che abbiamo considerato. Utile, per la prima metà del XX° secolo è stato il volume dei coniugi Woytinsky *"Word Population and Production",* XX Century Fundation, 1955, mentre particolarmente faticosa è stata la ricostruzione dell'andamento delle installazioni di telai a mano e meccanici, basato sul Mulahll *(Dictionary of Statistic, London 1898)* e sullo Smelser *(Social Change in the Industrial Revolution,* Routledge and Kegan, 1959); le storie economiche edite da Cambridge e da Fontana sono state tenute presenti per tutte le informazioni statistiche utili.

Un sistema esperto per la diagnosi di elaboratori

FRANCO TORQUATI

Honeywell Bull
Direzione Sistemi Esperti
Pregnana Milanese

1. Introduzione

L'articolo descrive la struttura di Sedel6[1], un sistema esperto a supporto dell'attività di diagnosi e manutenzione della famiglia di calcolatori DPS 6. Tale attività, articolata in una procedura di intervento, è illustrata in figura 1.

L'elevato numero di macchine e la loro diversificazione[2], oltre a rendere gravosa l'attività di assistenza agli utenti, evidenzia colli di bottiglia nella procedura d'intervento. Ciò è dovuto al fatto che le problematiche connesse alla diagnosi di un elaboratore sono di natura complessa e i tecnici coinvolti nell'attività di manutenzione non sempre possiedono le necessarie competenze.

Errori diagnostici in questa fase possono avere conseguenze negative in termini sia di costo che di immagine. Tra le altre ricordiamo:

- il persistere del blocco di macchina del cliente;
- un prolungato impegno del tecnico manutentore;
- la concentrazione del lavoro verso i tecnici di maggiore competenza;
- la sostituzione di parti a cui non è imputabile il malfunzionamento da rimuovere.

Per tali motivi è sentita l'esigenza di un sistema interattivo di supporto all'attività di diagnosi e manutenzione capace di mettere a disposizione conoscenze diversificate, distribuite fra vari specialisti e non sempre facilmente accessibili. L'obiettivo è l'incremento dell'autonomia del tecnico non specialista, accrescendo contemporaneamente l'accuratezza e la rapidità di intervento.

Il problema verifica la condizione iniziale che giustifica lo sviluppo di un sistema esperto in quanto il collo di bottiglia, e quindi i costi addizionali indotti, sono causati principalmente dalla disponibilità limitata delle competenze. Questo fatto, in-

(1) SEDEL6 è l'acronimo di Sistema Esperto Diagnostico per Elaboratori Livello 6.

(2) La famiglia DPS6 comprende 8 modelli, differenti per velocità di elaborazione e capacità di memoria, ed ha un'ampia diffusione sul mercato (oltre 6000 unità installate in Italia).

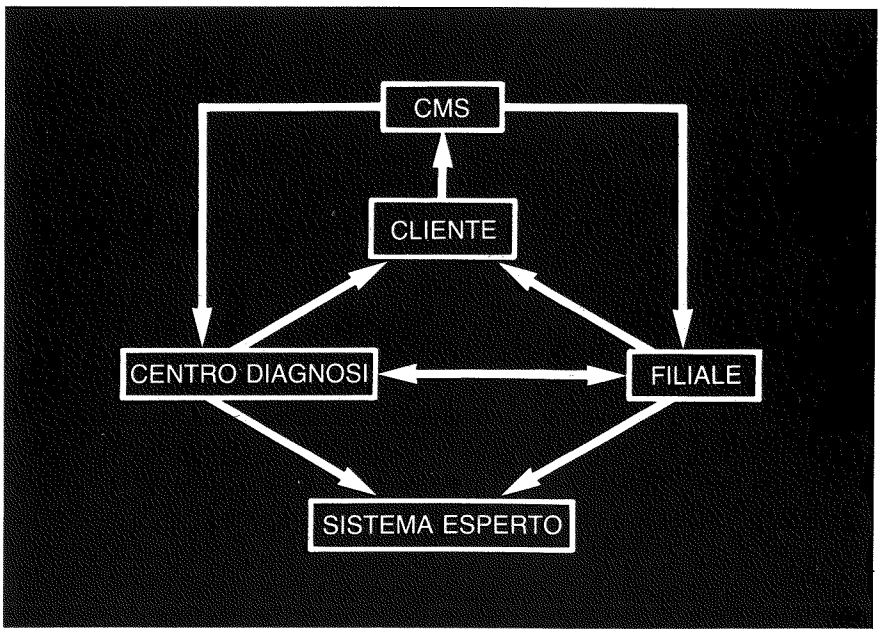


Figura 1 - L'ambiente operativo. CMS, acronimo per Call Management System, riceve le chiamate del cliente. Dopo una prima analisi, la richiesta di intervento viene passata (nel caso dei problemi più complessi) al Centro Diagnosi oppure alla Filiale competente. Centro Diagnosi e Filiale possono a loro volta chiamare il cliente oppure consultarsi fra di loro. Il sistema esperto è stato pensato come supporto all'attività dei tecnici del Centro Diagnosi e di Filiale.

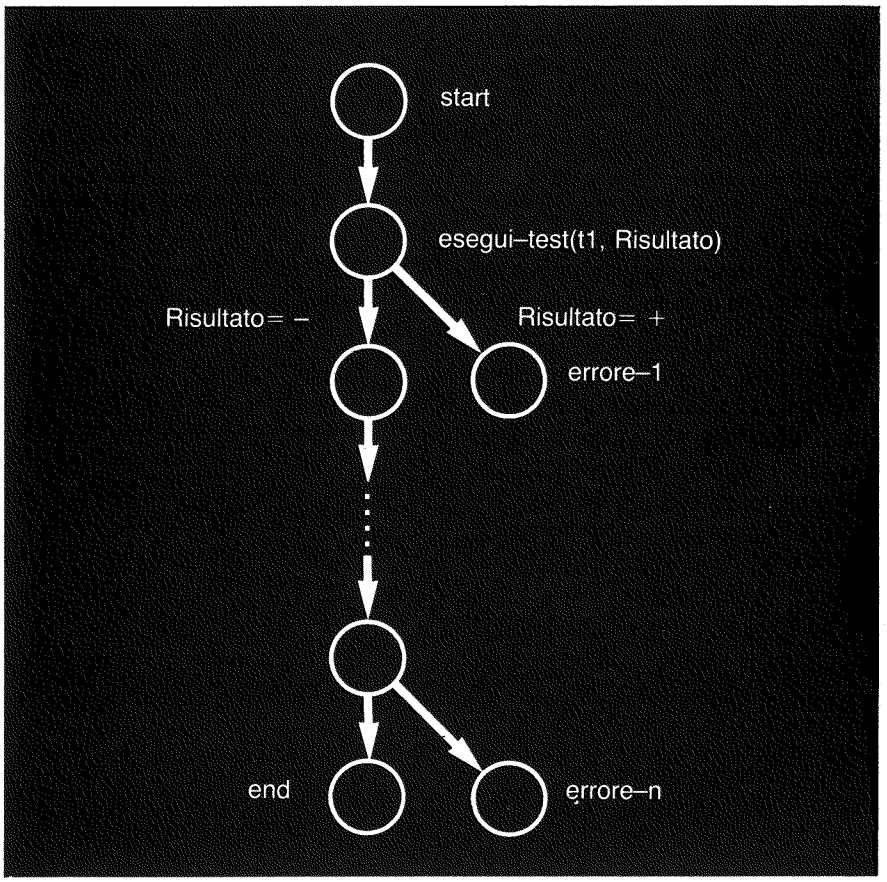


Figura 2 - Il metodo *start small* ha una struttura sequenziale. È utile, in ambiente di ingegneria e di fabbrica, per provare che un sistema è libero da errori. Il presupposto su cui si fonda, l'eliminazione del malfunzionamento prima di proseguire ulteriormente nel processo di diagnosi, lo rende efficace nel trattamento degli errori multipli. È però lento: per localizzare un errore è necessario provare (in media) n/2 componenti ed n può essere un numero grande.

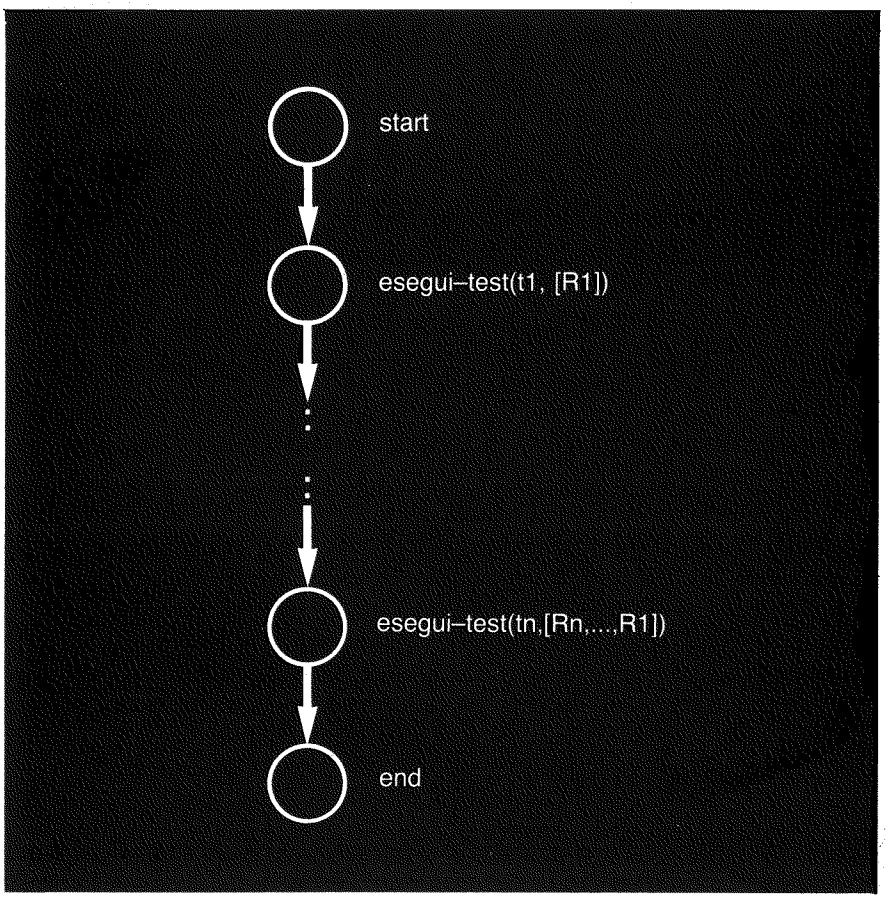


Figura 3 - L'approccio *multiple clue* ha una struttura simile a start small. I risultati delle varie prove sono accumulati in un file di output che viene prodotto in modo automatico e sottoposto all'esame dell'esperto.

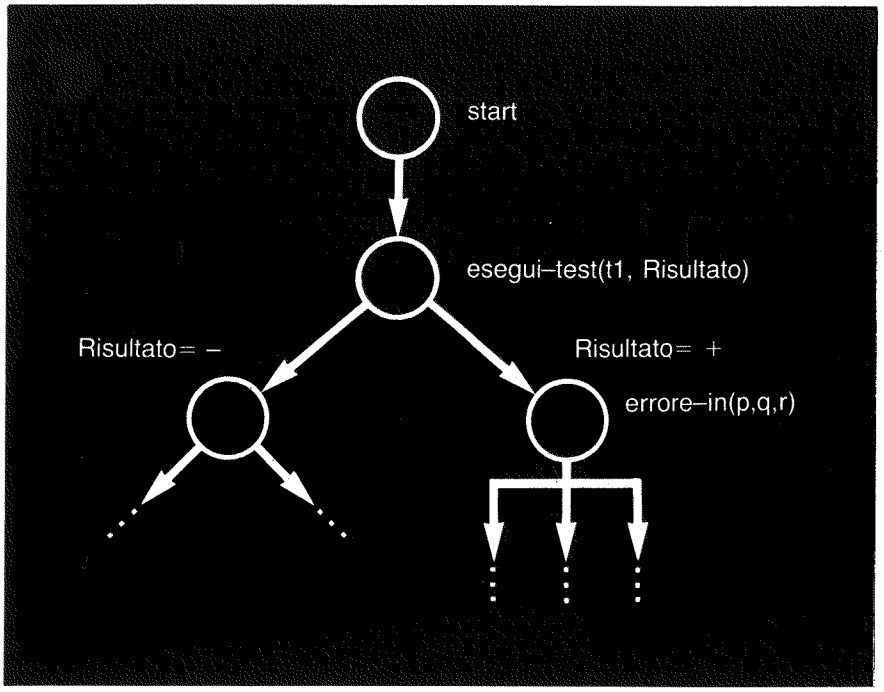


Figura 4 - L'approccio *start big* ha una struttura ad albero che permette di sveltire il processo di ricerca. Nello stato a cui è associato il goal esegui-test (t1, Risultato) tutte le componenti di macchina sono sospette. L'esecuzione del test permette di restringere l'indagine ad un sottoinsieme di tali componenti. Non sempre è possibile in modo deterministico decidere la prova successiva da eseguire. Quest'ultimo fatto è esemplificato nel disegno dalla struttura a pettine. In tale situazione possono essere solo fatte valere considerazioni statistiche: per es. prova a localizzare l'errore innanzitutto nel componente p, poi nel componente q infine nel componente r.

sieme all'analisi delle attività e delle conoscenze degli esperti, di cui parleremo nel prossimo paragrafo, ci ha fatto individuare in linguaggi e metodi di Intelligenza Artificiale lo strumento per la soluzione del problema.

2. Caratteristiche dell'attività diagnostica

Un elaboratore è una macchina complessa decomponibile in un insieme di moduli (hardware, firmware, software) variamente interconnessi tra loro. La difficoltà associate all'attività diagnostica sono dovute all'elevato numero di tali componenti e alle complesse interdipendenze che li legano. L'obiettivo del tecnico manutentore, durante il processo di diagnosi, consiste, in caso di guasto hardware, nell'isolamento del componente associato (Optimum Replaceable Unit), oppure nell'individuazione del segmento di codice che ha causato l'errore firmware o software.

Il raggiungimento di tale obiettivo non è facile in quanto il problema può avere svariate origini: dal programma utente all'hardware di sistema. Data la complessità del problema, di fronte ad un malfunzionamento non è ovvio dove incominciare l'indagine: è meglio investigare i sintomi di errore oppure tentare di ricrearne le condizioni? È meglio lanciare i programmi diagnostici e, in tal caso, lanciarli in sequenza ed in modo esaustivo oppure selezionare i diagnostici associati all'area sospetta?

Non ci sono risposte semplici a queste domande, tuttavia, in generale, possono essere individuati tre approcci metodologici distinti (vedi fig. 2,3,4) che di seguito elenchiamo.

Start small (detto anche a macchia d'olio)

Seguendo tale approccio si parte con il provare un sottoinsieme minimale del sistema e si procede quindi in modo incrementale. La difficoltà risiede nella scelta e nella sequenziazione dei test.

Multiple clue

L'analisi è basata sui risultati di una serie di prove consecutive che vengono portate avanti indipendentemente dal loro esito (positivo o negativo). Poiché un fallimento non determina la fine della catena delle prove, l'analisi del file di output può dar luogo a problematiche sofisticate.

Start big

L'analisi procede dal generale al particolare in modo dicotomico: l'esito di ciascun test seleziona la linea diagnostica successiva. È il metodo più veloce ma è anche complesso e soggetto ad errori.

Nel nostro caso, è ricostruibile, mediante interviste a specialisti, una strategia diagnostica di base facente uso, in modo promiscuo, delle tre metodologie.

Tale strategia, a meno che l'utente fornisca informazioni precise relative a guasti localizzati (il Card Reader non si accende, l'Unità a Nastro non si riavvolge, etc.) si articola in quattro passi fondamentali:

- verifica dei sintomi di guasto dell'alimentazione alternata e continua;
- esame dei sintomi di fallimento dei Quality Logic Test;
- controllo del percorso di caricamento del software;
- uso di procedure automatiche di testing (TACPAC).

I Quality Logic Test controllano le funzionalità del nucleo di macchina, il cui corretto funzionamento garantisce l'esecuzione e l'affidabilità delle procedure automatiche di test (TACPAC). La diagnosi del nucleo di macchina segue, anche se non in modo completo, l'approccio start small.

TACPAC (acronimo per Technical Assistance Center Performance As-

surance Check) è un sistema operativo software su disco, che genera ed elabora una sequenza di programmi di test e verifica e rilascia in output (se ve ne sono) la lista di errori prodotti. La lista è interpretata dal tecnico manutentore per isolare la causa del guasto. L'approccio è di tipo multiple clue.

L'approccio start big è applicato per l'isolamento rapido dell'area sospetta prima di procedere ad analisi di dettaglio mediante diagnostici automatici e procedure documentate. I tre approcci, per essere applicati efficacemente, richiedono:

- una rappresentazione strutturale del sistema al livello appropriato;
- una partizione del sistema in sottosistemi in funzione della rappresentazione strutturale;
- l'individuazione delle sequenze di input/output ai fini dell'isolamento del sottosistema o, ad un livello di granularità più fine, della componente malfunzionante;
- l'ordinamento dell'insieme dei test in funzione della struttura di macchina.

In particolare, il metodo start small, come già osservato precedentemente, si basa su una definizione dell'ordine in cui i vari controlli devono essere eseguiti che, partendo dal nucleo, sia lineare e ricoprente rispetto alle varie componenti di macchina. Multiple clue e start big, quest'ultimo in misura maggiore, richiedono un modo di procedere basato su considerazioni strutturali.

I punti riportati sopra elencano il tipo di conoscenze su cui si basa l'attività di diagnosi. Ciò che segue illustra, mediante un esempio, come le conoscenze diagnostiche vengono applicate:

"La macchina è in stato di "halt" e, poiché non stavano girando procedure utente, indaghiamo le cause in fase di inizializzazione.

Le cause possibili sono essenzialmente quattro: l'alimentatore è guasto oppure le sottofasi "initialize", "qlt" o "bootload" non sono andate a buon fine.

Procediamo a macchia d'olio e incominciamo con il verificare l'alimentatore.

Se le ventole non girano allora il guasto è da ricercarsi nella Power Distribution Unit, altrimenti controlla che...".

Il brano, estratto da una intervista ad un esperto, evidenzia i modi di ragionare ricorrenti durante una sessione diagnostica. Le caratteristiche principali riscontrabili sono essenzialmente tre:

- metodo classificatorio
- controllo non deterministico
- sequenzialità

Il metodo classificatorio riconduce fenomeni sconosciuti a membri di una classe conosciuta di oggetti o eventi. Tale processo è guidato da test ed osservazioni che isolano per gradi e tentativi la soluzione cercata. Se la soluzione tentativa riscontra delle inconsistenze con nuovi fatti accertati viene scartata e viene preso in considerazione un cammino alternativo (controllo non deterministico). Quando tutte le alternative ad un livello di specificazione sono state esaurite si riparte dal livello di specificazione immediatamente superiore.

L'ordine in cui i fatti vengono verificati è essenziale al processo di diagnosi. Infatti nell'ordinamento è contenuta sia informazione di tipo euristico (facilità di testing, maggior frequenza di guasto) sia informazione di tipo strutturale (se il componente A precede il componente B nel grafo strutturale, cioè l'output di A va in input a B, allora è verificato prima). Inoltre il significato dell'esito di un test è differente in dipendenza dalle azioni intraprese in precedenza.

Si considerino, ad esempio, i due differenti significati che nella procedura di verifica degli alimentatori ha il test sulla presenza di corrente continua nella lampadina corrispondente del pannello di controllo (cfr. [1]). In un contesto la presenza di corrente continua indica l'esistenza di un guasto nel componente "memory save", in un contesto differente permette di concludere che non ci sono malfunzionamenti nel sistema centrale di alimentazione.

3. Rappresentazione delle procedure diagnostiche

Lo sviluppo dei sistemi esperti ha reso popolare un nuovo stile di programmazione, differente da quello tradizionale basato in modo rigido sulla specifica della sequenza delle azioni da compiere ed in cui ogni azione può essere compresa, non da sola, ma nel contesto del programma preso nella sua globalità.

Al contrario, i linguaggi usati per la costruzione dei sistemi esperti permettono di rappresentare la conoscenza in modo dichiarativo mediante un insieme di fatti e di regole aventi un significato compiuto anche se staccati dal contesto di cui fanno parte.

È da notare tuttavia che il successo dei sistemi basati su regole è dovuto al fatto che la rappresentazione della conoscenza scelta è appropriata al tipo di problema che devono risolvere.

Ad esempio, la natura della conoscenza che sta alla base dei vari sistemi esperti applicati in campo medico è di tipo associativo, in quanto relaziona in modo più o meno diretto la rilevazione dei sintomi alla presenza degli stati patologici correlati. Tale correlazione può essere utilmente espressa mediante regole. Si consideri il seguente esempio tratto da Mycin, il prototipo dei sistemi esperti medicali, (cfr. [5]):

REGOLA 050
SE:
1) l'infezione è una batteremia primaria
2) la cultura batterica è tra quelle sterili
3) la sospetta via di ingresso è il tratto gastro-intestinale

ALLORA:
c'è una evidenza notevole (di valore 0.7) che l'organismo sia batterioide.

Mycin risolve il problema dell'identificazione di un organismo sconosciuto, ottenuto da colture di laboratorio, confrontando le informazioni messe a disposizione dall'utente con le proprie conoscenze sulle gerarchie di batteri. Ogni nodo in tale gerarchia rappresenta un'ipotesi di tipo batteriologico ed ogni sottoalbero dominato dal nodo i possibili sottotipi. Ogni ipotesi di tipo batteriologico è rappresentata mediante una regola.

In altri casi, però, la conoscenza di come risolvere un problema è data in modo procedurale come sequen-

za condizionata di azioni da intraprendere. Sebbene a priori non sia impossibile una rappresentazione di tipo dichiarativo, tuttavia il processo di traduzione può essere difficile e innaturale. Tale processo comporta infatti, in un modo o nell'altro, la codifica del controllo affinché regole o azioni siano eseguite nell'ordine voluto (cfr. [2]).

Ricordiamo che, nel nostro caso, è necessaria una rappresentazione esplicita del controllo, l'interpretazione dei sintomi essendo funzione del contesto e quindi dell'ordine delle azioni intraprese.

L'obiettivo che ci siamo proposti è stato quindi quello di formulare notazioni ed individuare strumenti capaci di rappresentare in modo adeguato la conoscenza procedurale, mantenendo tuttavia gli aspetti di chiarezza, modularitá ed elevata interattività caratteristici dei sistemi basati su regole.

Noi abbiamo assunto come punto di partenza per la rappresentazione della conoscenza lo schema degli automi (non deterministici) a stati finiti.

La teoria degli automi è evoluta in relazione a varie discipline. Costituita da un insieme di tecniche di natura algebrica e a volte logica, è stata concepita essenzialmente come calcolo dell'evoluzione dei processi discreti. Come tale offre un impianto concettuale, che noi abbiamo sfruttato, per la descrizione, lo studio delle proprietà e il controllo di procedure anche complesse.

Il modo forse più diffuso di descrivere una procedura fa uso dei diagrammi di flusso (flow-chart). Questo strumento, particolarmente utile quando si vuole mettere in evidenza la sequenza di azioni che compongono la procedura, è meno appropriato per esprimere la dipendenza delle azioni dagli input che le determinano. Per tale motivo è stato sviluppato uno strumento differente detto diagramma di transizioni.
Un diagramma di transizione descrive la struttura di un automa. Un automa è una macchina astratta che legge una sequenza di simboli di input e rilascia una sequenza di simboli di output. Un automa possiede un insieme di stati, ogni sequenza di input individua uno stato dell'automa ed ogni stato è rappresentato graficamente da un nodo del diagramma. Lo stato iniziale (unico) è individuato nel diagramma da una freccia entrante, gli stati finali da frecce uscenti. Una sequenza di simboli di input è accettata, partendo dallo stato iniziale, se fa accedere l'automa, per successivi cambi di stato, allo stato finale. L'insieme delle sequenze accettate definisce il linguaggio riconosciuto dall'automa.

Un diagramma di transizione è essenzialmente un grafo etichettato. Due nodi p e q di un grafo connessi da un arco orientato (freccia) con etichetta i/o indicano che il carattere di input i provoca un cambiamento di stato da p a q con rilascio di output o.
Un esempio di grafo di transizioni è dato in figura 5. Per una trattazione rigorosa della teoria degli automi cfr. [6].

I processi diagnostici che noi abbiamo considerato possono essere strutturati a due livelli mediante diagrammi specificanti rispettivamente:

1) transizioni fra contesti (vedi fig. 6). Per contesto si intende una procedura relazionata con la parte di macchina da verificare. Il grafo regola l'ordine di invocazione opportuno;

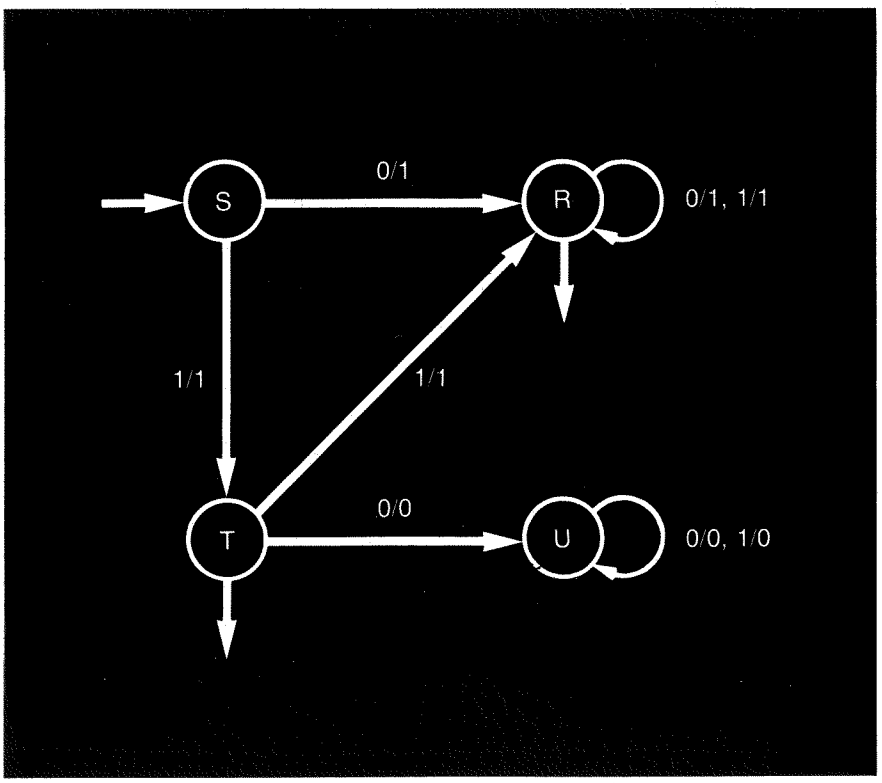


Figura 5 - Un esempio di macchina sequenziale. L'alfabeto di input e quello di output sono costituiti dall'insieme (0,1). Il linguaggio riconosciuto ($L = 1U0\Sigma^*U11\Sigma^*$, Σ [0,1]) è costituito dalle stringhe che iniziano con 0, 1, 11.
Un output uguale ad 1 indica che la porzione di stringa applicata allo stato iniziale e scandita sino al momento corrispondente è stata accettata. In altre parole l'automa si comporta come un programma interattivo che, carattere dopo carattere, asserisce il valore di verità della relazione di appartenenza della stringa scandita al linguaggio L.
Se il primo input è 0, l'automa passa dallo stato s allo stato r. L'output è 1, r è uno stato finale; quindi 0 è accettato come membro di L. A questo punto ogni sequenza di input applicata allo stato r lascia l'automa nello stato r e rilascia 1 come output. Quindi ogni stringa di input che inizia con 0 è accettata dall'automa. Questo rende conto della componente $0\Sigma^*$ di L. Procedendo in modo simile si possono giustificare le altre componenti del linguaggio.

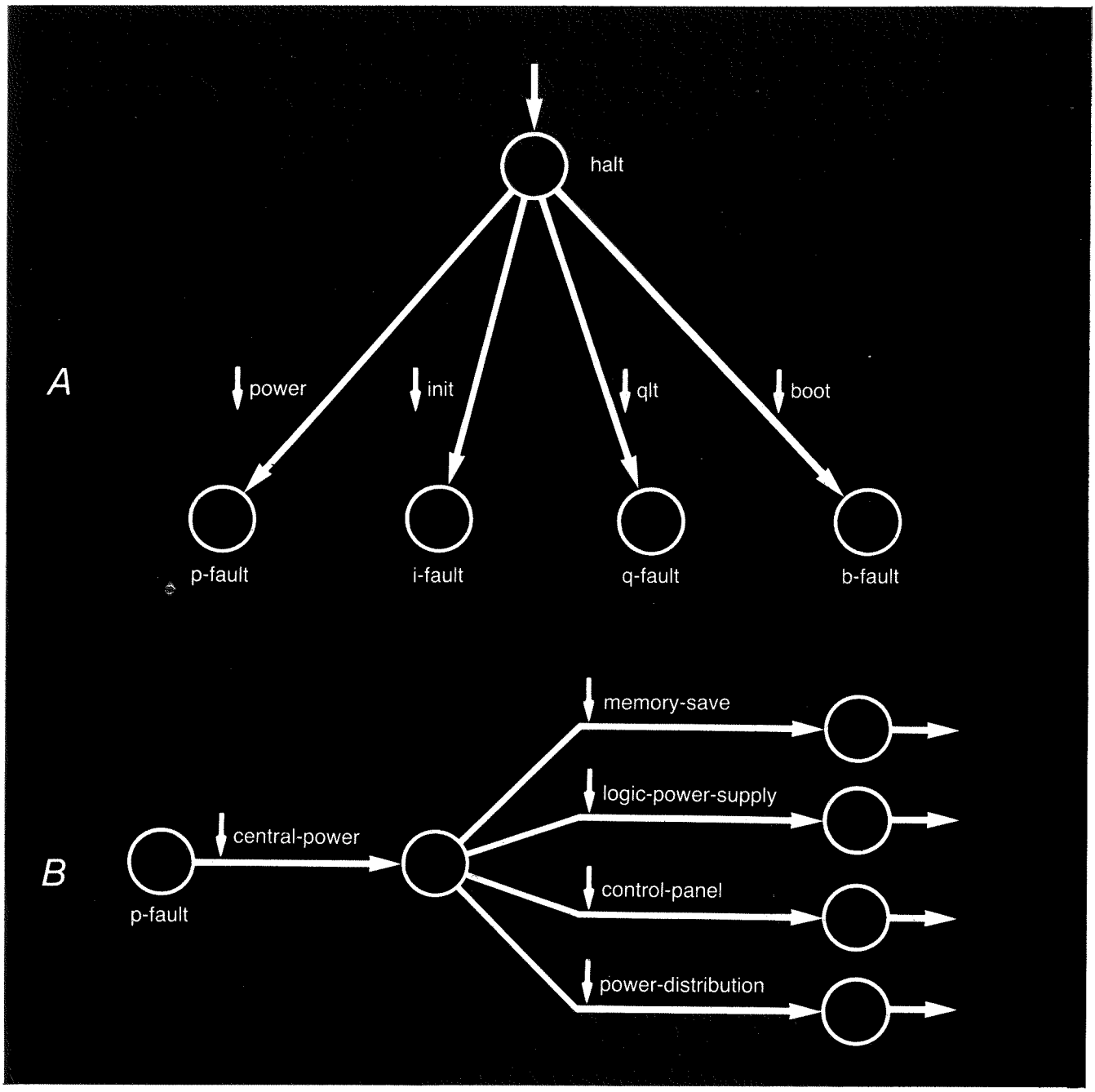


Figura 6 - I grafi che rappresentano rispettivamente le quattro possibili cause: (a) di un halt di macchina, (b) di un guasto nell'alimentatore centrale.

2) transizioni fra stati interni al contesto (vedi fig. 7). L'esecuzione di un contesto equivale al percorrimento di un grafo i cui nodi rappresentano lo stato diagnostico raggiunto e gli archi il valore di verità di un predicato (test) oppure una azione da compiere.

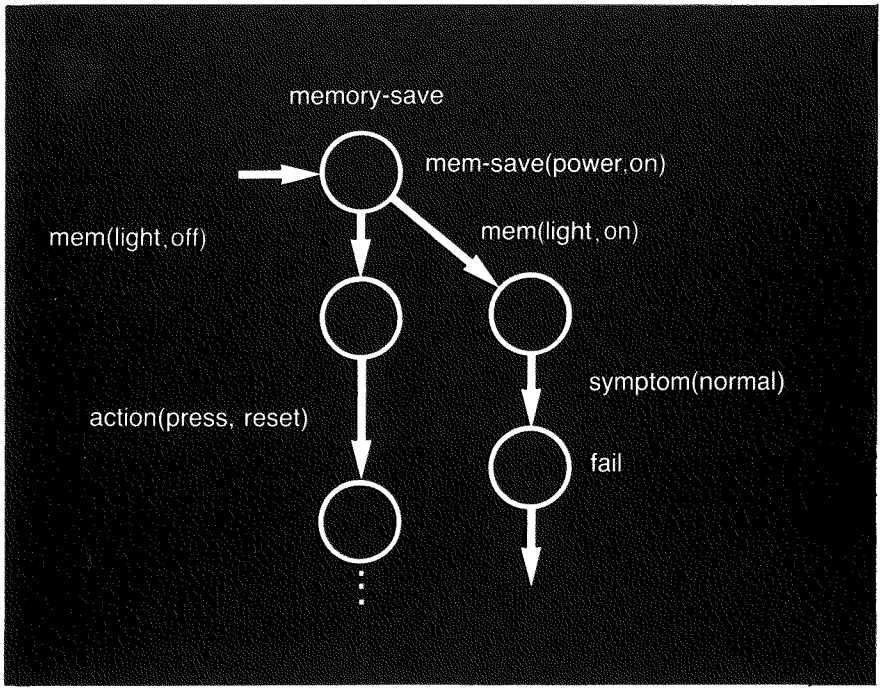
Tale schema ha un duplice vantaggio:

1) rappresenta in modo facile il controllo procedurale che può essere letto direttamente seguendo la successione degli archi che conduce dallo stato iniziale a quello finale;
2) permette di associare una semantica dichiarativa ad una procedura diagnostica, accumulando in ogni nodo l'insieme dei predicati verificati e delle azioni eseguite fino a quel momento.

In verità lo schema degli automi a stati finiti non è perfettamente adeguato, in quanto non permette transizioni fra stati guidate, a loro volta, da altre sottoprocedure diagnostiche. Il sistema ovvia a questa difficoltà implementando una estensione dagli automi a stati finiti comunemente chiamata RTN (Recursive Transition Networks) (cfr. [4]). Le RTN si rappresentano graficamente in modo del tutto simile agli automi tranne che gli archi possono essere etichettati a loro volta con il nome di altri automi la cui esecuzione condiziona il cambiamento di stato in oggetto.

In figura 6 la diagnosi di un halt di macchina è rappresentata mediante una RTN. In figura 6a lo stato inizia-

Figura 7 - Il contesto associato al modulo di memory-save. Agli archi sono associati predicati, azioni, messaggi. L'esecuzione di un contesto può fallire.



le (individuato dalla freccia entrante) ha quattro stati successivi. Poiché non è possibile mediante un singolo test operare una selezione univoca, il sistema, usando una strategia di tipo depth-first, attraversa da sinistra a destra i vari archi.
La freccia che punta verso il basso determina, mediante un meccanismo di tipo push-down, una chiamata di sottoprocedura ("Power" ad esempio). Power restituisce un valore oppure annuncia un fallimento. In tal caso il sistema invoca la procedura "Init". Altrimenti ricerca la componente dell'alimentatore centrale che ha causato l'halt di macchina (figura 6b).
Osserviamo esplicitamente che la possibilità di esprimere il controllo non deterministico, eliminando la necessità di sequenziare le varie procedure, aggiunge dichiaratività allo schema di rappresentazione scelto. Lo schema, inoltre, implica la possibilità di utilizzare le procedure, non come semplice guida per l'esecuzione, ma come oggetto mediante il quale è possibile calcolare

- lo stato del processo;
- gli stati successori;
- gli stati finali raggiungibili e i loro complementari;
- il cammino percorso.

Queste informazioni, date in modo astratto in termini di stati e cammini, hanno un significato rilevante per la comprensione e la corretta esecuzione delle procedure diagnostiche a cui siamo interessati.
Il complementare degli strati raggiungibili, nell'insieme degli stati finali, definisce, ad esempio, le cause di malfunzionamento che è possibile scartare dopo avere eseguito un insieme incompleto di prove.
Lo stato del processo definisce l'insieme dei predicati verificati e delle azioni compiute. Mediante il calcolo degli stati successivi è possibile spiegare il perché delle domande poste; il cammino percorso spiega infine il perché della conclusione raggiunta.

4. Interfaccia

Un sistema esperto per essere utile deve poter interagire con l'utente in modo naturale e flessibile, rispondere a domande riguardanti il comportamento del sistema e spiegare come le conclusioni sono state ottenute.
È noto che sistemi dotati di una base di conoscenze di notevole completezza e capaci di giungere a conclu sioni accurate e corrette non sono stati accettati con favore a causa di interfaccie inadeguate.
Nel nostro caso osserviamo che:

- la struttura sequenziale di un processo implica la memoria degli stati precedenti;
- la realizzazione mentale di tale memoria, essenziale per la comprensione del processo, diventa un compito arduo col crescere della complessità della funzione computata.

Come conseguenza, la costruzione di un sistema che si limiti a riprodurre le sequenze di domande documentate in una procedura offre all'utente un'interfaccia opaca in relazione al perché delle domande poste e al come è associata la diagnosi finale alla sequenza delle risposte fornite dall'utente. A questo punto si può far notare che anche le procedure diagnostiche meglio documentate non contengono giustificazioni esplicite che aiutino il tecnico nella loro comprensione e corretta utilizzazione. Tali caratteristiche negative, costituenti una evidente sorgente di errori, possono essere rimosse avendo a disposizione un sistema che garantisca la visibilità della logica di diagnosi.
In figura 8 sono illustrati cinque momenti di una sessione diagnostica guidata da Sedel6. Nella finestra principale è ospitato il dialogo tra l'utente ed il sistema sotto forma di domande o menu e relative risposte. Le altre finestre, aperte in dipendenza dalle chiavi comando digitate, ospitano alternativamente:

- le sequenze di cicli diagnostici completati;

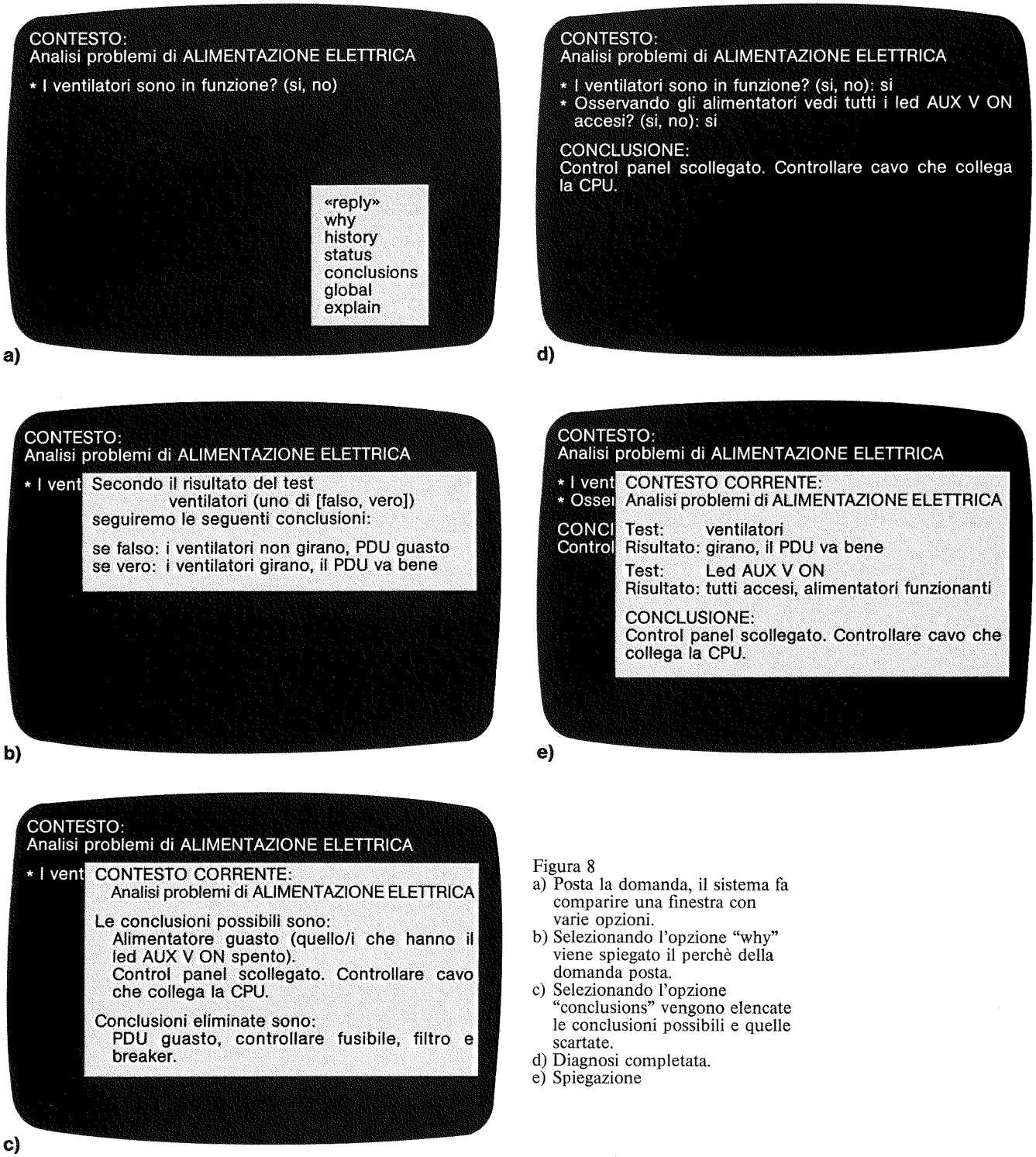


Figura 8
a) Posta la domanda, il sistema fa comparire una finestra con varie opzioni.
b) Selezionando l'opzione "why" viene spiegato il perchè della domanda posta.
c) Selezionando l'opzione "conclusions" vengono elencate le conclusioni possibili e quelle scartate.
d) Diagnosi completata.
e) Spiegazione

- il percorso completato all'interno del ciclo diagnostico in atto;
- spiegazioni a domande e conclusioni;
- le variabili con i valori assegnati;
- la lista, in dipendenza dello stato, delle diagnosi possibili e di quelle scartate.

Il sistema inoltre controlla il tipo dei dati di input e offre la possibilità di retrazione qualora siano introdotti dati errati.

5. Conclusioni

Sedel6 è stato sviluppato su un calcolatore Sun-2 è rilasciato su PC Honeywell Bull con sistema operativo MS DOS. È stato scritto interamente in Prolog, linguaggio che ha permesso una implementazione elegante e semplice delle idee architetturali esposte (vedi Appendice). Le transizioni che costituiscono una procedura sono state rappresentate in modo dichiarativo mediante fatti e separatamente è stato scritto il motore inferenziale che simula il comportamento di un tecnico che tali procedure applica. Rispetto ad un approccio di tipo tradizionale, facente uso, ad esempio, di Pascal, si possono evidenziare almento tre vantaggi:

- la rappresentazione di una procedura mediante fatti Prolog è molto più compatta ed uniforme rispetto

a quella fornita da un linguaggio procedurale basato su side-effects;

- la separazione della base delle conoscenze dal motore inferenziale consente di mettere in luce le informazioni implicite nel flusso di controllo;
- tale separazione favorisce una rappresentazione della conoscenza esplicita e facilmente modificabile.

Il risultato è un sistema con un maggior grado di flessibilità e, per quanto riguarda la base delle conoscenze, manipolabile dall'esperto di settore in modo autonomo.

6. Ringraziamenti

L'autore ringrazia R. Pea, E. Tedeschi e G.C. Ghiselli della Direzione Servizio Clienti della Honeywell Bull, per la collaborazione e il supporto fornito. Ad essi è dovuta l'idea di sviluppare Sedel6.

Appendice

Un programma Prolog acronimo per PROgramming in LOGic, (cfr. [3]), è una sequenza di clausole, ogni clausola essendo una implicazione della forma

B if A1 and ... and An.

Ciascun Ai, al pari di B, è il nome di un predicato (o relazione) seguito da una lista di termini (T1, T2, ..., Tn) (gli argomenti del predicato). Un termine è una costante, una variabile oppure, recursivamente, un nome di predicato seguito da una lista di termini. È convenzione Prolog indicare le variabili con lettera iniziale maiuscola e nomi di predicati e costanti con lettera iniziale minuscola. Una clausola può essere letta come una implicazione preceduta da un quantificatore universale che si applica a tutte le variabili della clausola. Ad esempio la clausola.

```
transd (In, Out) if
        initial (State) and
        transd (State, In, Out).
```

può essere letta nel seguente modo:

per ogni In,Out,State

Out è il flusso di output rilasciato da transd a fronte del flusso di input In

if

State è uno stato iniziale

and

Out è l'output rilasciato da transd a fronte dell'input In a partire dallo stato State.

Le clausole con antecedente vuoto sono dette fatti o asserzioni.

È possibile specificare in Prolog un automa a stati finiti mediante tre relazioni

1) una relazione unaria finale che definisce gli stati finali;
2) una relazione unaria initial che definisce gli stati iniziali;
3) una relazione quaternaria trans

```
trans (State,Next,In,Out)
```

fra quattro variabili denotanti rispettivamente: lo stato attuale, lo stato successivo, l'input che determina la transizione e l'output rilasciato.

Consideriamo come esempio l'automa di figura 5. Esso puo essere specificato creando un file, che chiameremo automa, contenente i seguenti fatti

```
trans(s,r,0,1).
trans(s,t,1,1).
trans(r,r,1,1).
trans(r,r,0,1).
trans(t,u,0,0).
trans(t,r,1,1).
trans(u,u,0,0).
trans(u,u,1,0).
final(r).
final(t).
initial(s).
```

Inoltre è possibile scrivere un programma transd, che, relazionando il flusso di input In con il flusso di output Out (In ed Out sono nomi di liste), definisce il comportamento di un automa astratto.

Il programma è definito da tre clausole

```
transd (In,Out) if
        initial (State) and
        transd (State, In, Out).
transd (State, [I:S], [O:R]) if
        trans (State,Next,I,O) and
        transd (Next,S,R).
transd (State,[ ],[ ]) if
        final (State)
```

La prima clausola pone l'automa nello stato iniziale. Quindi il programma itera leggendo gli elementi del flusso di input. In particolare:

- se il primo elemento nel flusso di input è I unifica il primo elemento della stringa di output O con l'output O di una transizione trans attivata da I nello stato State e quindi chiama se stessa a partire dallo stato successivo Next;
- esaurito il flusso di input, il processo termina se è stato raggiunto uno stato finale.

Archiviamo il programma in un file che chiameremo comportamento. Ora diamo da interpretare all'interprete Prolog l'unione dei file automa e comportamento. Il risultato è una macchina virtuale, costruita so-

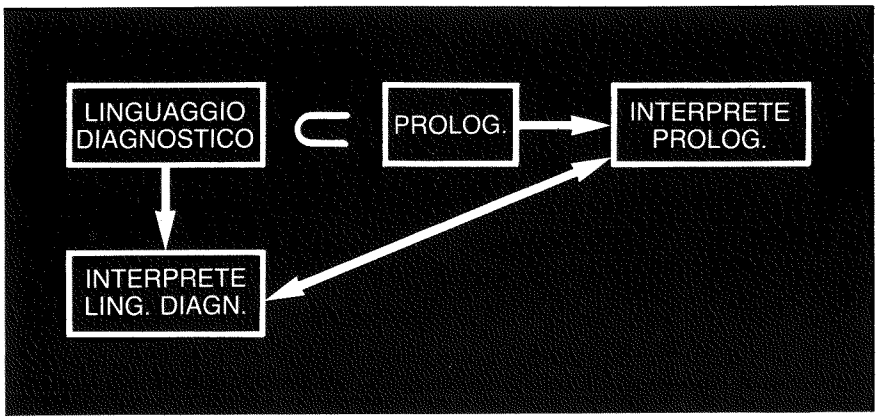


Figura 9 - Il motore inferenziale, in Sedel 6, è più esattamente definito come interprete per un Linguaggio Diagnostico. L'interprete, scritto in Prolog, è a sua volta interpretato dall'interprete Prolog.

pra Prolog, che simula il comportamento dell'automa specificato nel file automa. Rimpiazzando il contenuto di questo file è possibile avere a disposizione i simulatori degli automi corrispondenti.

L'esempio dato mostra una caratteristica dei sistemi esperti: la separazione della base di conoscenze dal motore (inferenziale) e l'aumento corrispondente di flessibilità raggiunto tramite il concetto di astrazione.

Anche il nostro sistema segue questo modello. Le singole transizioni che rappresentano gli elementi della conoscenza diagnostica sono espresse in termini Prolog mediante una sintassi semplice da noi definita (Diagnostic Language).

Le relazioni dell'interprete, di cui transd è il germe, con l'ambiente sono illustrate in figura 9.

7. Riferimenti bibliografici

[1] DPS6 *Troubleshooting & Repair Procedures,* Customer Services Division Honeywell, 1983.

[2] Micheal P. Georgeff & Amy L. Lansky *Procedural Knowledge,* in Proceedings of the IEEE, october 1986, pp. 1383-98.

[3] Ivan Bratko, *Prolog Programming for Artificial Intelligence,* Addison-Wesley, 1986.

[4] Patrick H. Winston, *Artificial Intelligence,* Addison-Wesley, 1984.

[5] Bruce G. Buchanan, Edward H. Shortliffe, *Rule-Based Expert Systems,* Addison-Wesley, 1984.

[6] Samuel Eilenberg, *Automata, Languages and Machines* Vol. 1, Accademic Press, 1974.

La crittografia a chiave pubblica

R. BORTOLAMEAZZI, L. FELICIAN, L. SABBADINI

Istituto di Matematica, Informatica e Sistemistica
Università di Udine

1. Introduzione

I sistemi di comunicazione elettronici in rapido sviluppo nella società moderna sono caratterizzati da grande velocità e precisione e da costi in continua diminuzione, ma presentano anche seri problemi di sicurezza.

Per proteggere le imponenti quantità d'informazione riservata - come registrazioni di operazioni bancarie o cartelle cliniche che oggi sono registrate nelle banche di dati automatiche - si può ricorrere ai cifrari, o crittosistemi, cioè a metodi per cifrare, ossia trasformare, l'informazione, in modo da renderla incomprensibile e quindi inutile a chi non sia autorizzato ad accedervi.

In un sistema crittografico il testo in chiaro, o "plaintext", viene trasformato secondo certe regole nel testo in cifra, o "ciphertext". Tale operazione si chiama cifratura. Il "ciphertext" viene quindi spedito a destinazione tramite un opportuno canale di trasmissione, del quale, tuttavia, non ci si può fidare: lungo il percorso può essere appostata una spia, la quale può intercettare il "ciphertext" e tentare di decifrarlo. Anche il destinatario legittimo decifra il "ciphertext" e riottiene il "plaintext": se il cifrario è ben congegnato l'operazione di decifrazione può risultare piuttosto semplice al destinatario, ma di complessità proibitiva alla spia. Ciò è possibile perchè il destinatario legittimo conosce certe informazioni che devono rimanere del tutto inaccessibili alla spia e che perciò non devono venire affidate al canale poco sicuro usato per trasmettere i crittogrammi.

Tali informazioni costituiscono la chiave del cifrario.

Si definisce *crittologia* lo studio di sistemi di comunicazione segreti. Tale disciplina si suddivide in due parti tra loro competitive:

- la *crittografia,* che si occupa della costruzione di crittosistemi efficienti e rappresenta la parte costruttiva della crittologia;
- la *crittoanalisi,* che studia i possibili attacchi ai crittosistemi (cioè le operazioni di decifrazione senza aver a disposizione la chiave) e ne rappresenta la parte distruttiva.

A tutt'oggi i matematici non dispongono di un mezzo per dimostrare la sicurezza computazionale di un sistema, e la storia della crittografia insegna come troppo spesso sistemi creduti inattaccabili avessero invece difetti nascosti. É auspicabile che gli sviluppi della teoria della complessità riescano infine a fornire gli strumenti necessari a costruire crittosistemi di cui si possa dimostrare la sicurezza computazionale e nei quali si possa garantire l'assenza di "pecche" nascoste.

Fino ad allora un gruppo di problemi matematici caratterizzati da un certo tipo di intrattabilità computazionale serviranno da base per una nuova classe di procedimenti di cifratura che vengono detti cifrari o crittosistemi a chiave pubblica.

2. Sistemi crittografici

I sistemi di crittografia si basano su algoritmi che si dividono in tre classi (come si può vedere in figura 1):

- algoritmi simmetrici
- algoritmi a una via
- algoritmi asimmetrici

Una differenza sostanziale tra queste tre classi di sistemi risiede nell'uso e nella forma delle chiavi. La chiave per crittografare è analoga ad una chiave per casseforti: il meccanismo della serratura rappresenta l'algoritmo di cifratura/decifrazione.

Ciascuna delle tre classi di sistemi di crittografia è distinta dalle altre per il tipo di algoritmo impiegato, che a sua volta è strettamente correlato al numero e tipo/i di chiave/i in uso.

Sistemi simmetrici

Il più noto sistema di crittografia è basato sull'ampia classe degli algoritmi simmetrici. Esempi di algoritmi simmetrici sono il DES, il "Caesar Cipher", un certo numero di cifrari della II Guerra Mondiale, ed i cerchi decodificatori segreti. I sistemi simmetrici hanno dominato quindi la crittologia sin dall'inizio delle comunicazioni segrete.

Benchè gli algoritmi simmetrici differiscano notevolmente tra loro nel progetto e nella realizzazione, tutti hanno un'esigenza comune: la chiave usata per decrittografare deve essere la stessa usata per crittografare. Si tratta cioè di un sistema ad una chiave. Questa è la classica chiave da

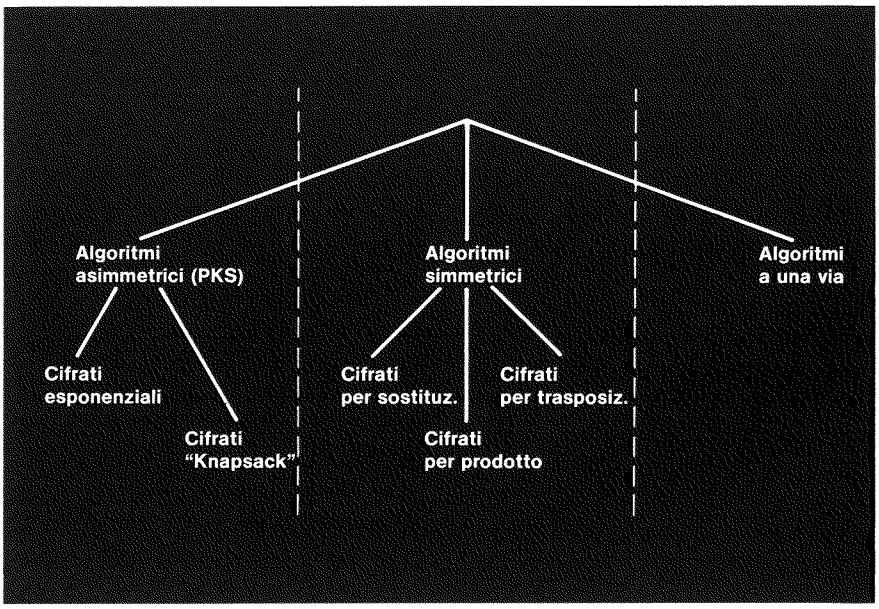


Fig. 1 - Le classi di algoritmi impiegati in crittografia.

cassaforte così come la conosciamo: la stessa chiave usata per chiuderla è quella necessaria per aprirla.

Sistemi ad una via

Gli algoritmi ad una via possono soltanto crittografare. Essi sono prontamente ottenibili e sono qui menzionati solo per ragioni di completezza. Il loro principale uso è per una memorizzazione sicura dell'informazione di accesso al sistema.

Sistemi asimmetrici

La classe più recente della crittografia è il PKS (Public Key System). Essa è anche chiamata asimmetrica, dato che sono richieste due chiavi diverse per realizzare una trasformazione completa dal "plaintext" al "ciphertext" e viceversa. Di norma una chiave viene usata per crittografare e l'altra, in qualche modo ad essa correlata, realizza il processo inverso. Ciò è analogo al caso di una cassaforte che richieda una chiave particolare per essere chiusa ed una seconda, derivata in qualche modo dalla prima, per aprirla,

I PKS sono nati da un tipo di matematica chiamata "teoria della complessità", che consente di valutare la quantità di tempo (e, quindi, di denaro) richiesto per calcolare numericamente le soluzioni di particolari problemi. Si tratta, cioè, di un progetto che rende la sicurezza delle informazioni dipendente da un problema di calcolo che, al momento attuale, necessita di quantità proibitive di tempo e/o denaro per essere risolto.

Tale progetto si basa sulle cosiddette funzioni unidirezionali: funzioni invertibili tali per cui il calcolo della funzione diretta sia "facile", mentre quello della funzione inversa sia "difficile".

Sono stati proposti diversi PKS, ma ricadono generalmente in due categorie: il "knapsack" e gli algoritmi "esponenziali" (RSA).

La gestione delle chiavi di comunicazione

Vi sono due importanti considerazioni che si accompagnano alla realizzazione di un sistema crittografico. Una è la scelta dell'algoritmo, basata su disponibilità, efficienza, sicurezza e costo computazionale dello stesso. L'altra è la memorizzazione protetta delle chiavi.

L'ultimo aspetto è denominato "gestione delle chiavi" e viene considerato come il problema più difficile da risolvere. La sicurezza dell'informazione crittografica è adeguata soltanto quanto lo è la sicurezza della chiave usata per decrittografarla. Se la chiave viene resa incidentalmente o volontariamente nota, l'informazione comunicata ritorna sotto tutti gli aspetti ad essere un "plaintext". Purtroppo mittente e destinatario possono non essere a conoscenza del fatto che il loro sistema sia stato compromesso, così da continuare, erroneamente, a scambiarsi importanti informazioni.

3. La gestione delle chiavi nei sistemi simmetrici

L'esempio che segue illustra il problema più importante in merito alla gestione delle chiavi presentato dagli algoritmi simmetrici nel contesto delle comunicazioni.

Il mittente X, per esempio, desidera trasmettere un messaggio al destinatario Y (fig. 2).

Un canale di comunicazione li mette in collegamento. Il destinatario riceve il "ciphertext" del mittente, ma senza la chiave corretta avrà a sua disposizione un'informazione senza senso. Il sistema allora funziona solo se disponiamo di un canale speciale, assolutamente fidato, destinato alla trasmissione della chiave che deve essere spedita dal mittente al destinatario prima che essi inizino a comunicare.

A questo punto potrebbe venir spontanea una domanda: visto che non c'è possibilità di intercettazione, perchè non trasmettere direttamente, sul canale speciale, il "plaintext"?

In realtà, le dimensioni della chiave sono di norma più ridotte di quelle del "plaintext": un'unica chiave relativamente breve viene impiegata

per smaltire un traffico di messaggi piuttosto intenso. Inoltre l'uso del canale speciale che non è soggetto ad intercettazioni potrebbe essere costoso, oppure il canale potrebbe essere disponibile solo per intervalli di tempo troppo brevi per trasmettere l'intero messaggio.

Avvenuto lo scambio della chiave, entrambi gli utenti possono pensare di garantirsi la propria segretezza. Naturalmente se uno o l'altro rivelasse la chiave, ogni "ciphertext" trasmesso sarebbe potenzialmente passibile di manomissione. Questa necessità di scambiarsi la chiave prima delle trasmissioni del "ciphertext", così come la necessità di segretezza, sono spesso citati come i due difetti del sistema simmetrico convenzionale di crittografia.

Verranno ora analizzati alcuni esempi di cifrari simmetrici.

L'algoritmo DES

Il DES (Data Encription Standard) è un cifrario in cui la funzione di cifratura/decifrazione utilizza sostituzioni e trasposizioni tra esse correlate. Ogni messaggio viene suddiviso in blocchi di 64 bit ($x_0,...,x_{63}$), ognuno dei quali viene trasformato in un blocco di 64 bit di "ciphertext" ($y_0,...,y_{63}$) tramite una chiave di 56 bit ($k_0,...,k_{55}$). I restanti 8 bit della chiave sono di parità. Lo spazio delle chiavi contiene 2^{56} chiavi diverse e ci sono 2^{64} blocchi di 64 bit di "plaintext".

Si usa la notazione DES (k,x) per indicare la cifratura del blocco di "plaintext" x utilizzando la chiave k, e la notazione DES^{-1} (k,y) per indicare la decifrazione del blocco di "ciphertext" y usando sempre la chiave k.

L'algoritmo DES è definito solo per blocchi di "plaintext" x lunghi 8 byte. Quindi:

$<x> = (x_1,...,x_m)$

m = numero di blocchi

dove

$x_i = (x_{i,0}\ x_{i,1}...x_{i,63})$

è un blocco di 8 byte $(1 \leq i \leq m)$

Il modo ovvio per cifrare un "plaintext" di m blocchi, ciascuno di 8 byte, è quello di applicare il DES ad ogni blocco, come segue:

$<y> = (y_1,...,y_m)$

$y_j = DES\ (k,x_j)$ $(1 \leq j \leq m)$

Questo uso del DES è ideale perchè è possibile decrittografare solo alcune parti di "ciphertext", senza dover eseguire l'operazione per l'intero file. Ciò deriva dal fatto che blocchi di "plaintext" identici sono cifrati in blocchi di "ciphertext" identici (con la stessa chiave). Così "plaintext" con pattern ripetuti hanno "ciphertext" con pattern ripetuti. Per impedire che questa particolare struttura possa essere d'aiuto per decifrare un "ciphertext", viene aggiunta un'ulteriore operazione: il "chaining", che maschera le ripetizioni nei blocchi di "plaintext".

Cifrario a sostituzione

Si supponga di voler cifrare il seguente messaggio:

LA QUIETE DOPO LA TEMPESTA

Fissiamo una permutazione delle lettere dell'alfabeto (la chiave del cifrario) come quella che segue:

ABCDEFGHILMNOPQRSTUVZ

OCSATUPLVEIDQFBHZGMRN

(nella seconda riga compaiono tutte le 21 lettere, ognuna una sola volta).

La regola di cifratura è semplice: si sostituisce ogni lettera del "plaintext" con la corrispondente lettera che sta nella riga in basso della permutazione: la A con la 0, la B con la C ecc. Il "ciphertext" risultante è:

EO BMVTGE AQFQ EO GTIFTZGO

La regola di decifrazione è ovvia, basta usare la permutazione inversa, che si ottiene "capovolgendo" la permutazione diretta:

OCSATUPLVEIDQFBHZGMRN

ABCDEFGHILMNOPQRSTUVZ

Si può subito notare che il numero di chiavi possibili è 21!, che è un numero di 19 cifre decimali. In questo modo la ricerca esauriente della chiave, per forzare il cifrario, diventa sconsigliabile.

Un cifrario di questo tipo può essere forzato utilizzando tecniche di tipo statistico (frequenza delle lettere, considerazioni di tipo semantico, ecc.).

L'esperienza dice che "ciphertext" con 30 lettere sono decifrabili.

Se è noto a priori che i messaggi sono molto brevi, allora i cifrari a sostituzione risultano perfetti. In realtà è necessario trasmettere grandi quantità di informazioni e quindi questo cifrario risulta inefficiente.

Un'obiezione però va fatta per quanto riguarda i tentativi di attacco al "ciphertext": se sono al più neces-

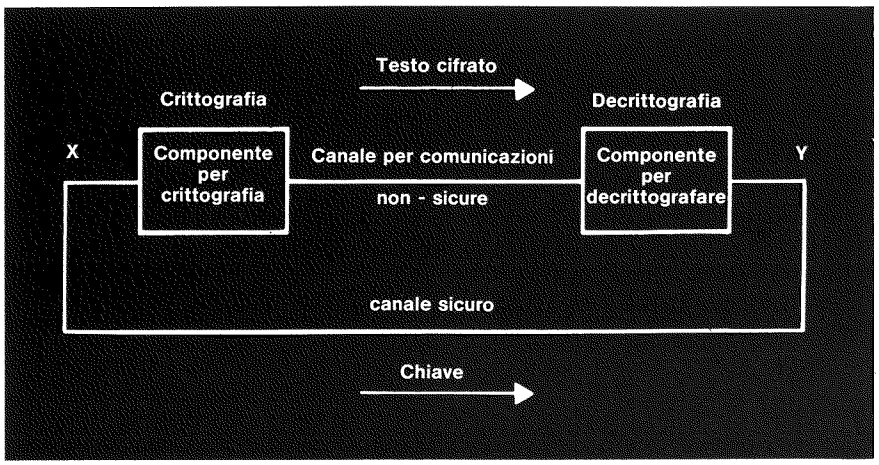


Fig. 2 - Trasmissione separata della chiave e del testo in un sistema crittografico.

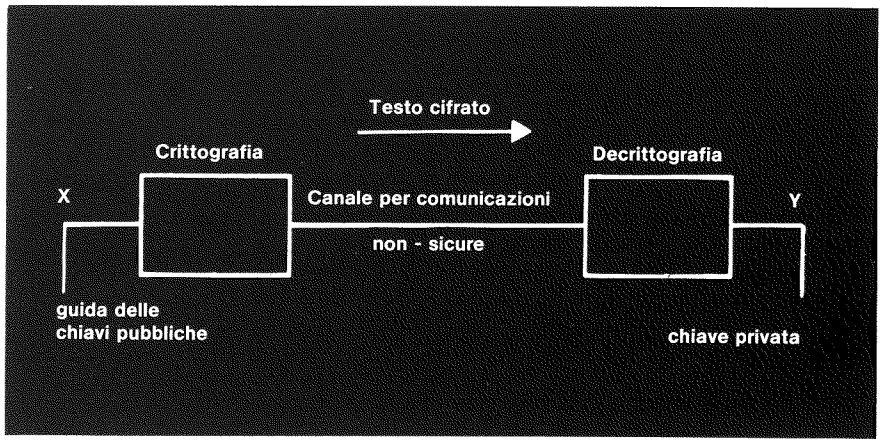


Fig. 3 - Trasmissione del testo cifrato in un sistema a chiave pubblica.

sari 21! tentativi per forzarlo è indispensabile sapere che si è di fronte al "ciphertext" ottenuto mediante un cifrario a sostituzione. L'intercettatore, cioè, oltre alla chiave deve anche conoscere il sistema di cifre che è stato utilizzato.

Nella crittografia strategica si fa allora un'ipotesi pessimistica: si suppone che l'intercettatore conosca il sistema di cifre usato (in pratica questo non è sempre vero).

Cifrario a trasposizione

Si basa sul principio dell'anagramma.

Si fissa un numero intero P (periodo del cifrario). Si considera una permutazione degli interi compresi tra 1 e P: questa permutazione costituisce la chiave di cifratura. Le possibili chiavi sono in numero pari a P!

Supponiamo, ad esempio, di scegliere P = 7 e di fissare la permutazione:

1 2 3 4 5 6 7

4 6 3 5 7 1 2

Il messaggio viene allora spezzato in blocchi di lunghezza P e le P lettere di ciascun blocco vengono rimescolate, o anagrammate, in base alla permutazione: in ogni blocco in "ciphertext" si scrivono la quarta, la sesta, la terza, ..., la seconda lettera del corrispondente blocco in "plaintext".

Il "ciphertext" corrispondente a

LA QUIET/E DOPO LA/ TEMPEST/A

è allora

UE QITLA/P LOOA ED/PSMETTE/A

(le barre che separano i blocchi sono state scritte solo per comodità).

Anche in questo caso, per decifrare si usa la permutazione inversa:

4 6 3 5 7 1 2

1 2 3 4 5 6 7

Rispetto al "plaintext" le lettere sono le stesse nel "ciphertext" anche se compaiono con un ordine diverso. La frequenza delle lettere è la stessa e quindi un'analisi statistica basata su questo parametro non è di aiuto al crittoanalista.

4. La gestione delle chiavi nei sistemi asimmetrici

Nei sistemi PKS (Public Key System) vengono usate due chiavi, una per crittografare e l'altra per decrittografare. Fatto rilevante è che la chiave usata per crittografare può essere resa pubblica. Ciò è possibile poichè, in teoria, la chiave per decrittografare corrispondente (privata) è impossibile a calcolarsi o da dedurre da quella pubblica. L'esempio precedente (fig. 2), del mittente X che invia un "ciphertext" al destinatario Y, può essere riesaminato nel contesto di un PKS (fig. 3).

Entrambi hanno realizzato lo stesso tipo di PKS e ciascuno può crittografare messaggi usando la chiave pubblica dell'altro, ottenuta da una guida resa disponibile al pubblico.

Quando l'uno o l'altro riceve un messaggio crittografato, usa la sua chiave privata per decrittografarlo. Dato che non si è avuto uno scambio di chiave prima delle comunicazioni, non è richiesto un canale sicuro a priori.

Ad un primo esame sembra che i due difetti dei sistemi simmetrici siano stati evitati. Non è necessario stabilire un canale sicuro per scambiare una chiave - questa funzione è già stata svolta attraverso la guida pubblica - e la rivelazione della chiave privata di qualcuno crea dei rischi soltanto a quella singola parte (della coppia di interlocutori coinvolti).

Certamente il PKS appare migliore di un sistema simmetrico; in realtà, gestire chiavi in reti di grandi dimensioni usando ambedue i tipi di algoritmi è più complesso che nell'esempio precedente.

L'algoritmo RSA

Questo sistema a chiave pubblica basa la sua sicurezza sull'utilizzo della fattorizzazione di un numero grande, ovvero della ricerca di tutti i suoi fattori primi. Un numero primo è un intero divisibile solo per 1 e per se stesso. Questo problema è stato studiato fin dal tempo degli antichi greci ma, nonostante alcuni progressi, la fattorizzazione di un numero di 200 cifre terrebbe occupato il più veloce degli attuali calcolatori elettronici per circa un miliardo di anni. Tanto per fare un esempio più abbordabile, consideriamo la scomposizione del numero 29083.

Procedendo a mano, si giungerebbe, dopo almeno un'ora, a scoprire i due unici fattori di questo numero 127 e 229.

Per verificare che si tratta dei fattori corretti, invece, è sufficiente meno di un minuto; ciò suggerisce che il problema della fattorizzazione possa costituire un buon punto di par-

tenza per la costruzione di una funzione unidirezionale.

Escogitare il modo di introdurvi una molla segreta è senz'altro difficile, ma gli ostacoli sono stati superati da Rivest, Shamir e Adleman, che hanno ideato il sistema RSA (dalle loro iniziali).

Il messaggio deve essere anzitutto codificato in forma numerica ponendo, per esempio, A = 1, B = 2 ecc.

Un utente A del sistema RSA crea la sua chiave in questo modo:

- sceglie, in modo casuale, due numeri primi, p e q, sufficientemente grandi (ad esempio 100 cifre decimali);
- calcola il valore di n = p x q;
- sceglie poi, sempre in modo casuale, un intero D, grande, che non abbia divisori comuni nè con p-l nè con q-l;
- calcola E come l'inverso di D modulo (p-l)x(q-l);
- a questo punto, rende nota, come sua chiave pubblica, la coppia (E, n) e conserva, come sua chiave segreta, la coppia (D, n).

Chiunque, allora, può crittografare un messaggio M da mandare ad A utilizzando la chiave pubblica di A e ottenere il "ciphertext" corrispondente utilizzando l'equazione:

$C = M^E \bmod n$

Allo stesso modo A può decrittografare il "ciphertext" C mediante l'equazione:

$M = C^D \bmod n$

Si consideri il seguente esempio.

Siano p = 47 e q = 59, si ottiene, quindi, n = 2773.

Se si sceglie D = 157, si può calcolare E = 17.

La chiave pubblica sarà allora (E, n) = (17, 2773) e la chiave segreta (D, n) = (157, 2773).

Il messaggio M=31 potrà essere crittografato, utilizzando la chiave pubblica, nel "ciphertext" $C = 31^{17} \bmod 2773 = 587$.

Decrittografando si otterrà il "plaintext" originale $M = 587^{157} \bmod 2773 = 31$.

Il cifrario a chiave pubblica RSA, come ricordato sopra, si basa sul fatto che, sebbene sia semplice, sotto il profilo computazionale, trovare dei numeri primi elevati, la scomposizione del prodotto di due numeri siffatti è a tutt'oggi di computazione irrealizzabile. È importante tenere presente che esistono algoritmi efficienti per determinare se un numero è primo e ciò risulta molto più facile della scomposizione in fattori primi di un numero delle stesse dimensioni.

Per chiarire come venga ricavata la chiave di decifrazione, è necessario considerare il numero (p-l)x(q-l), un oggetto ben noto in teoria dei numeri, chiamato funzione di Eulero. Questa funzione, che viene indicata con $\varphi(n)$, è definita come il numero di interi tra 1 e n che non hanno fattori comuni con n. Non è difficile vedere che se n è uguale a pxq, allora $\varphi(n)$ è uguale a (p-l)x(q-l). È stato introdotto il numero $\varphi(n)$ in quanto, per le funzioni che, come quella usata nel sistema RSA per cifrare, sono calcolate modulo n, l'aritmetica degli esponenti non viene eseguita modulo n, bensì modulo $\varphi(n)$.

Consideriamo ad esempio l'espressione 2^{11} modulo 10.

Poichè 2^{11} è uguale a 2048, che diviso per 10 da come resto 8, l'espressione è uguale a 8.

Si noti che se il calcolo viene eseguito riducendo in primo luogo l'esponente modulo 10, non si giunge al risultato corretto; infatti 11 modulo 10 e 1, e 2^1 è 2. D'altra parte 10 è uguale a 2x5, sicchè $\varphi(10)$ è uguale a (2-1)x(5-1), ossia 4. Poichè 11 modulo 4 è uguale a 3, calcolando 2^{11} modulo 10 riducendo dapprima l'esponente modulo 4, si ottiene la risposta corretta, cioè 2^3, ossia 8.

Ora, le proprietà di $\varphi(n)$ garantiscono che esiste sempre un inverso moltiplicativo D di E, modulo $\varphi(n)$; vale a dire ExD modulo (p-1)x(q-1) è uguale a 1. In effetti c'è sempre un metodo di calcolo veloce e semplice per ricavare D. (Non è difficile vedere che nell'esempio fatto sopra, dove p è 5, q è 11 ed E è 3, (p-1)x(q-1) è uguale a 40 e D a 27, dato che 3x27 supera di uno 2x40). Questo inverso D è la prima componente della chiave di decifrazione segreta per il sistema RSA. In altri temini, elevando il "ciphertext" alla D-esima potenza e riducendolo modulo n si riottiene il "plaintext",

Dunque, nel sistema RSA, il ricorso al modulo ha una duplice funzione: non solo impedisce la ricostruzione della chiave di decifrazione (D, n) a partire dalla chiave pubblica (E, n), ma il suo impiego nell'algoritmo di cifratura previene la possibilità di un ritorno diretto dal ciphertext" al "plaintext". La difficoltà di calcolare D a partire dall'informazione pubblica (E, n) deriva dalla difficoltà di fattorizzare n, di ricavare cioè p e q.

Ancora una volta l'esempio dato è troppo piccolo per garantire una effettiva sicurezza, ma dato che la scomposizione di un numero grande costituisce un problema veramente arduo, la difficoltà di forzare il crittosistema aumenta molto rapidamente al crescere di n. Quando p e q sono presi in modo che n abbia circa 200 cifre, la decifrazione diventa impossibile, da un punto di vista computazionale, per chiunque non sia il destinatario previsto. Se da una parte il procedimento di decifrazione (senza l'informazione segreta) deve essere inattuabile, dall'altra il procedimento pubblico di cifratura e quello privato di decifrazione devono essere effettuabili sotto il profilo computazionale. A tutta prima l'impiego pratico del sistema RSA, a questo proposito, sembra comportare alcuni problemi.

Consideriamo il semplice esempio in cui il numero M = 2 del "plaintext" sia stato trasformato nel numero cifrato C = 8. Per applicare l'algoritmo di decifrazione $M = C^D \bmod n$ è necessario calcolare 8^{27} modulo 55 (che infatti è uguale a 2). Moltiplicare 8 per se stesso 27 volte costituisce peraltro un'operazione ingombrante che coinvolge numeri molto elevati e moltissime operazioni elementari. In un sistema RSA pratico, in cui D potrebbe essere un umero di circa 200 cifre, questa procedura diverrebbe irrealizzabile anche su un calcolatore molto potente.

Fortunatamente esiste un modo più rapido di calcolare simili funzioni. In primo luogo si utilizza lo sviluppo binario dell'esponente (cioè si espri-

me l'esponente come la somma di potenze di 2) per scomporre la funzione nel prodotto di fattori minori.

Per esempio, 27 è uguale 1+2+8+16, da cui otteniamo che 8^{27} è uguale a $8x8^2x8^8x8^{16}$. Calcolando quindi prima i fattori più piccoli, e facendone poi il prodotto, si riduce il numero delle operazioni richieste. Così, 8^2 modulo 55 può venire calcolato con un'unica moltiplicazione modulare (una moltiplicazione ordinaria seguita da una divisione ordinaria), visto che 8x8=64 modulo 55 è uguale a 9. Quindi 8^4, che è $(8^2)x(8^2)$, è valutabile con una ulteriore operazione modulare 9x9 = 81 modulo 55 = 26 e così via. (Sostituendo il valore 8 modulo 55, cioè 9, nei fattori più grandi, si evita che i numeri nel calcolo diventino troppo grandi). Per calcolare 8^{27} sono dunque sufficienti sette moltiplicazioni modulari: quattro per valutare 8^2, 8^4, 8^8, e 8^{16} e altre tre per moltiplicare 8 per 8^2 per 8^8 per 8^{16}.

Anche quando D ha 200 cifre questo metodo fornisce un procedimento di decifrazione molto efficiente, che richiede al massimo 1330 operazioni modulari, contro le 10^{200} operazioni necessarie nell'impostazione diretta.

5. Conclusione

Nella società dell'informazione in cui siamo ormai entrati, la riservatezza dei dati costituisce un aspetto fondamentale. Le tecniche crittografiche avranno, quindi, un impiego sempre più esteso. Tra esse, quella "a chiave pubblica" costituisce la soluzione più promettente, per lo meno per quanto riguarda le applicazioni commerciali.

6. Bibliografia

[1] Ald, S.G. *"Digital Signature: A Tutorial Survey."* Computer 16 (2), 1983.

[2] Brickell, E.F. *"A Fast Modular Multiplication Algorithm with Applications to Two-Key Cryptography."* Advances in Cryptology - Proceedings of CRYPTO 1982.

[3] Deming, D.E.R. *"Cryptography and Data Security."* Addison-Wesley, Reading, Mass., 1982.

[4] Diffie, W. and Hellman, M. *New Directions in Cryptography."* IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976.

[5] Ehrsam, W.F., Matyas, S.M., Meyer, C.H. *"Cryptography."* IBM System Journal, Vol. 17, No. 2, 1978.

[6] Garey, M.R. and Johson, D.S. *"Computers and Intractability: A Guide to the Theory of NP-Completeness."* W.H. Freeman & C. 1979.

[7] Goodman, R.M.F. and McAuley, A.J. *"A New Trapdoor Knapsack Public-Key Cryptosystem."* Department of Electronic Engineering, University of Hull, 20 July 1984.

[8] Graham, S.L. and Rivest, R.L. *"Secure Communication over Insecure Channels."* Communications of the ACM, Vol. 21, April 1978.

[9] Hellman, M.E. *"La Crittografia a Chiave-Pubblica."* Le Scienze, No. 137, Dicembre 1979.

[10] Herlestam, T. *"Critical Remarks on Some Public-Key Criptosystem."* BIT 18:4, 1978.

[11] Kochanski, M. *"Developing an RSA CHIP."* Business Simulation Ltd.

[12] Knuth, M.E. *"The Art of Computer Programming, Vol. 2: Seminumerical Algorithms."* Addison-Wesley, Reading, Mass., 1969.

[13] Konheim, A.G., Mack, M.H., Mc-Neill, R.K., Tuckerman, B., Waldbaum, G. *"The IPS Cryptographic Programs."* IBM System Journal, Vol. 19, No. 2, 1980.

[14] Lagarias, T.C. *"Performances Analysis of Shamir's Attack on the Basic Merkle-Hellman Knapsack Cryptosystem."* AT&T Bell Laboratories, Murray Hill, New Jersey.

[15] Meijer, H. and ACK, S.G. *Digital Signature Schemes."* Cryptologia, Vol. 6, No. 4, October 1982.

[16] Merckle, R.C. and Hellman, M.E. *"Hiding Information and Signatures in Trapdoor Knapsacks."* IEEE Transactions on Information Theory, September 1978.

[17] Meyer, C. and Matyas, S.M. *"Cryptography - A New Dimension in Computer Data Security."* Joh Wiley & Sons, New York, 1982.

[18] Miyaguchi, S. *Fast Encryption Algorithm for the RSA Cryptographic System."* Proceedings COMPCON 1982.

[19] Pollard, J.M. *"Theorems on Factorization and Primality Testing."* Proc. Camb. Phil. Soc. 76 (1974).

[20] Popek, G. and Kline, C. *"Encryption and Secure Computer Networks."* ACM Computing Surveys, vol. 11, No. 4, December 1979.

[21] Purdy, G. *"A High-Security Log-In Procedure."* Communications of the ACM, August 1974.

[22] Rieden, R.F., Snyder, J.B., Widman, R.J., Barnard, W.J. *"A Two Chip Implementation of the RSA Public-Key Encryption Algorithm."* Digest of Papers for the 1982 Government Microcircuit Applications Conference (November 1982).

[23] Rivest, R.L. *"A Description of a Single-Chip Implementation of the RSA Cipher."* Lambda 1 (Fourth Quarter 1980).

[24] Rivest, R.L., Shamir, A., Adleman, L. *"A Method of Obtaining Digital Signatures and Public-Key Cryptosystem."* Communications of the ACM, Vol. 21, No. 2, February 1978.

[25] Rivest, R.L. *"Optimal Arrangement of Keys in a Hash Table."* JACM 25:2, April 1978.

[26] Rivest, R.L. *"RSA Chip (Past/Present/Future)"* MIT Laboratory for Computer Science.

[27] RSA Security, Inc. *"Preliminary Data Sheet for the RSA Cryptochip."* 1984.

[28] Schwartz, M. *"La Crittografia a Chiave-Pubblica."* Sistemi e Automazione, No. 262, Settembre 1985.

[29] Sgarro, A. *"Crittografia."* Muzzio Editore, Agosto 1986.

[30] Simmons, G.J. and Norris, M.J. *"Preliminary Comments on the M.I.T. Public-Key Cryptosystem."* Criptologia, October 1977.

Didattica col computer: una sperimentazione

G. CANEPA, G. GARAVAGLIA
Honeywell Bull
Direzione Formazione
Milano

1. Introduzione

L'articolo presenta una esperienza didattica coll'elaboratore, orientata alla scuola media superiore.

Il nostro scopo non era di realizzare un intero corso, ma di sviluppare un singolo argomento da usare come banco di prova per verificare strategie didattiche, metodologie di sviluppo, linguaggi e strumenti software.

In un'ottica generale, l'obiettivo era di evidenziare, attraverso uno sviluppo specifico, le potenzialità peculiari dell'elaboratore quando viene utilizzato a scopo didattico.

Come veicolo della sperimentazione si è scelto un argomento di fisica, l'ottica geometrica, su cui è stata sviluppata una intera lezione.

Nell'articolo vengono illustrati i criteri seguiti nella realizzazione ed i risultati ottenuti dalla sperimentazione.

2. Impostazione della sperimentazione

Il primo problema affrontato è stata la scelta di una metodologia da seguire nello sviluppo della lezione.

La metodologia scelta si basa su due concetti fondamentali: a) la definizione di un preciso ciclo di sviluppo da seguire nella produzione del "courseware", b) l'utilizzo in alcune fasi di questo ciclo di diverse competenze fornite da diversi esperti (esperto della materia, esperto nell'uso dei media, esperto di didattica, esperto CAI...).

Il ciclo di sviluppo è mostrato in fig. 1. Esso non si discosta molto dal ciclo di vita normale di un qualsiasi software; l'unica fase realmente diversa è la seconda, in cui vengono decise le strategie didattiche.

Per quanto concerne gli esperti, ci siamo avvalsi della collaborazione, sia in fase di progettazione che di verifica del lavoro svolto, di un docente di fisica di un Istituto Tecnico Superiore e di un esperto di tecniche CAI dell'Istituto di Tecnologie Didattiche del CNR di Genova; la loro consulenza è stata di valido aiuto sia nella costruzione della lezione che nella verifica della validità didattica della lezione stessa.

La seconda scelta da compiere riguardava l'argomento di fisica da trattare e quale tipo di applicazione sviluppare (tutoriale, simulazione, dialogo, problem solving...).

La scelta dell'argomento (ottica geometrica, in particolare riflessione e rifrazione), suggerita dall'esperto della materia, risponde ad una effettiva necessità poichè, di norma, la dotazione di laboratorio delle nostre scuole non permette un'analisi adeguata di fenomeni quali, ad esempio, la rifrazione della luce.

Come impostazione del lavoro abbiamo scelto un approccio di tipo simulativo, prima di tutto perchè questo tipo di applicazione ben si adatta a materie come la fisica e poi perchè l'argomento attiene a esperienze di laboratorio più che alla descrizione verbale di fenomeni.

La sperimentazione è stata, inoltre, orientata dal fatto che il campione di studenti disponibili per il test provenivano da un Istituto Tecnico Superiore. Ciò ha avuto un riflesso sul programma, in quanto gli studenti che sono stati sottoposti all'esperimento non avevano ancora affrontato lo studio della trigonometria, per cui la legge della rifrazione anzichè in funzione dei seni degli angoli di incidenza e di rifrazione è stata espressa in funzione dei segmenti corrispondenti ai seni dei due angoli.

Infine, un breve cenno agli strumenti software usati per lo sviluppo della lezione. Si tratta del Sistema Didattico CAN-8, distribuito dalla Honeywell Bull, che permette un approccio abbastanza agevole alla composizione di corsi mediante moduli CAI e che offre la possibiltà di utilizzare un linguaggio autore per la codifica dei programmi didattici.

3. Strategie didattiche

Nello sviluppo di materiale CAI, oltre ai contenuti della lezione, va prestata molta attenzione anche al modo in cui questi contenuti vengono proposti; bisogna cercare infatti di sfruttare, per mezzo di accurate scelte didattiche, tutte le capacità offerte dal mezzo in modo da creare lezioni che abbiano una buona interattività, che prevedano una certa individualizzazione del processo formativo, che non annoino lo studente, ma al contrario lo coinvolgano e stimolino la sua attenzione.

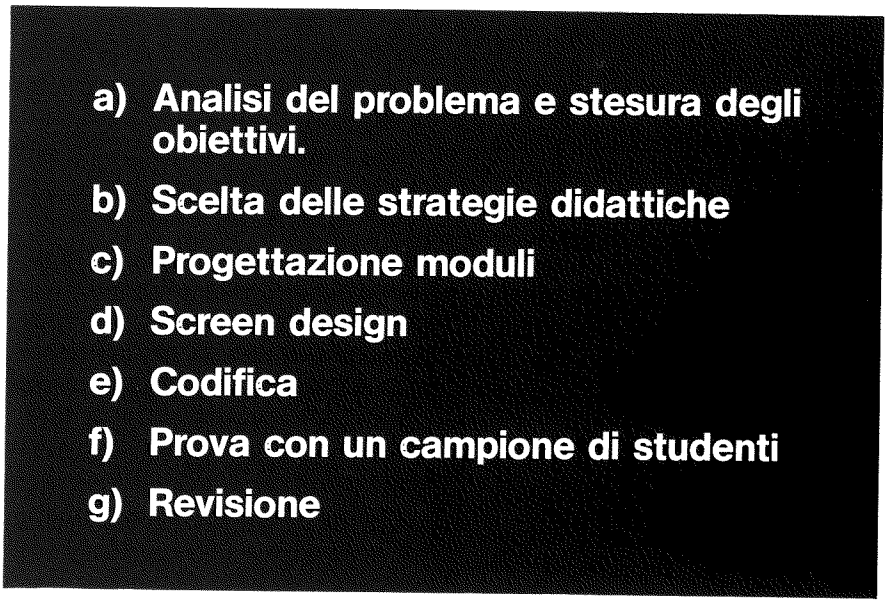


Fig. 1 - Ciclo di sviluppo di un software didattico.

Le strategie didattiche da noi scelte per lo sviluppo del programma "Ottica" cercano appunto di tener conto di questi obiettivi di base e si possono riassumere in tre scelte fondamentali: a) una impostazione del lavoro di tipo completamente sperimentale, b) l'utilizzo di simulazioni semplici ed allo stesso tempo significative, c) l'introduzione di alcune fasi di gioco per favorire il coinvolgimento dello studente.

Per quanto riguarda il primo punto, abbiamo scelto di impostare la lezione su un metodo sperimentale diviso in tre fasi: 1) una serie di simulazioni di esperimenti, 2) una raccolta di dati mediante misurazione, 3) presentazione dei dati raccolti e scoperta della legge per mezzo di un ragionamento su di essi.

Questo tipo di impostazione si è rivelato molto utile: in primo luogo perchè lo studente, in questo modo, oltre alle nozioni specifiche, apprende un "metodo" da applicare ad una vasta gamma di fenomeni fisici; in secondo luogo perchè lo studente non riceve una legge o una formula calata dall'alto, ma la scopre attraverso una serie di passaggi logici e ciò gli permette di capire più a fondo il significato della legge stessa.

Per quanto riguarda invece il secondo punto della strategia didattica, esiste una difficoltà obiettiva nello scegliere il tipo di simulazione da proporre.

Occorre infatti usare delle simulazioni che siano di facile comprensione, ma che allo stesso tempo, abbiano tutti i dettagli necessari. Occorre, cioè, che, siano guidate da meccanismi di immediata comprensione ed allo stesso tempo siano aderenti, nei particolari, alla realtà.

Nel programma "Ottica" si è cercato di dare priorità alla semplicità di guida e di comprensione delle simulazioni, in modo che gli studenti possano concentrare la loro attività mentale sui risultati dell'esperimento e sui collegamenti logici esistenti tra questi risultati.

Il terzo punto della strategia didattica prevede invece l'inserimento di una componente ludica nel programma, per alleggerire in alcuni momenti il lavoro. In effetti, il gioco può essere visto come parte del processo didattico, e alcune attività che, a prima vista, possono sembrare inutili ai fini dell'apprendimento, contribuiscono anch'esse alla formazione dello studente (ad es. il tiro al bersaglio che permette di simulare i percorsi fatti dalla luce nel caso della rifrazione, consente allo studente di avere un'idea intuitiva di come, al cambiare dell'angolo di incidenza, cambi l'angolo di rifrazione).

Ovviamente si è cercato di collocare queste fasi di gioco nei momenti più ripetitivi della lezione, nei momenti cioè in cui più facilmente subentra la noia, la disattenzione; ciò ha permesso di trasformare questi momenti critici in momenti didattici, in cui lo studente, apprende senza accorgersene.

4. Il programma "Ottica"

Il programma "Ottica" comprende 4 capitoli: 1) velocità della luce, 2) riflessione della luce, 3) rifrazione della luce, 4) esercizi.

L'obiettivo del primo capitolo è di mostrare allo studente come la luce, a seconda del mezzo in cui viaggia (aria, acqua, vetro, quarzo, diamante ecc...), si muova con velocità diverse.

La simulazione usata per raggiungere questo obiettivo è basata su delle "gare di velocità" fra raggi di luce posti in mezzi differenti (fig. 2). I raggi di luce devono percorrere la stessa distanza (A-B = 4.500.000 km) e lo studente, prima dello svolgersi della prova, è invitato a fare una previsione sul risultato. Dopodichè partono i due raggi ed è così possibile rendersi conto visivamente di come, in realtà, vadano le cose. Dopo ogni prova vengono fornite le velocità della luce, sia per il primo che per il secondo mezzo. A questo punto lo studente sceglie se effettuare un'altra prova o vedere la tabella in cui sono riportate le velocità relative ai vari mezzi presi in considerazione.

Va sottolineato che in questa simulazione si è fatto in modo che le velo-

cità dei raggi siano veramente proporzionali ai mezzi attraversati.

Questa prestazione è stata ottenuta creando una routine che non solo muove un raggio più velocemente dell'altro, ma li muove in modo tale che il ritardo temporale tra un raggio e l'altro sia quello reale su una distanza pari a quella tra A e B.

Il secondo capitolo vuole invece portare lo studente alla scoperta della legge della riflessione, cioè del fatto che quando un raggio di luce incide su una superficie parte della luce viene riflessa e l'angolo che il raggio riflesso forma con la normale alla superficie è esattamente uguale all'angolo formato dal raggio incidente con la stessa normale.

Lo studente ha a disposizione un meccanismo per lanciare dei raggi di luce da una sorgente S con l'angolazione desiderata; egli deve colpire un bersaglio B, facendo riflettere il raggio di luce su di uno specchio (fig. 3a).

Quando viene premuto il tasto [f], una routine disegna sia il raggio incidente sia il raggio riflesso; in questo modo è possibile vedere se il colpo ha avuto successo o meno (fig. 3b).

Lo studente può provare e riprovare fino a colpire il bersaglio, oppure può richiedere la soluzione, cioè il valore dell'angolo che permette di colpire B.

Quando B viene colpito, viene eseguita una specie di fotografia della situazione per poter misurare le grandezze in gioco (fig. 3c).

Lo studente a questo punto deve scegliere cosa misurare (le possibilità sono 10: i sei segmenti ed i quattro angoli); le grandezze prescelte per la misurazione verranno misurate anche in tutti gli esperimenti successivi, in modo da costruire una tabella con i valori di queste grandezze al variare della posizione del bersaglio e quindi al variare dell'angolo di incidenza.

Fig. 2 - Esempio di "gara di velocità" tra raggi di luce in mezzi diversi (vuoto e acqua).

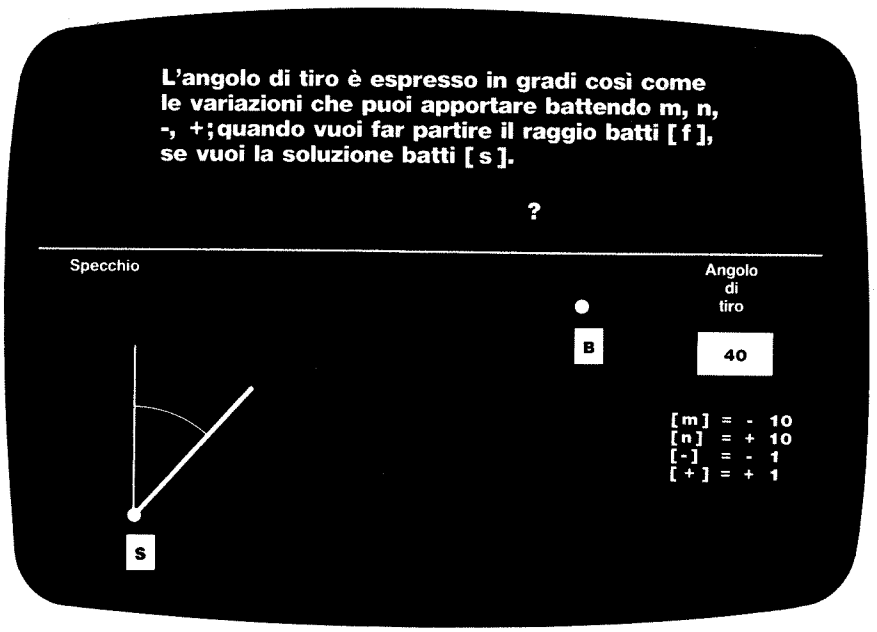


Fig. 3a - Inizio della simulazione dell'esperimento sulla riflessione. Lo studente deve colpire il bersaglio B lanciando un raggio di luce dalla sorgente S contro lo specchio. È possibile variare l'angolo di tiro utilizzando i comandi sulla destra e non vi è limite al numero dei tentativi.

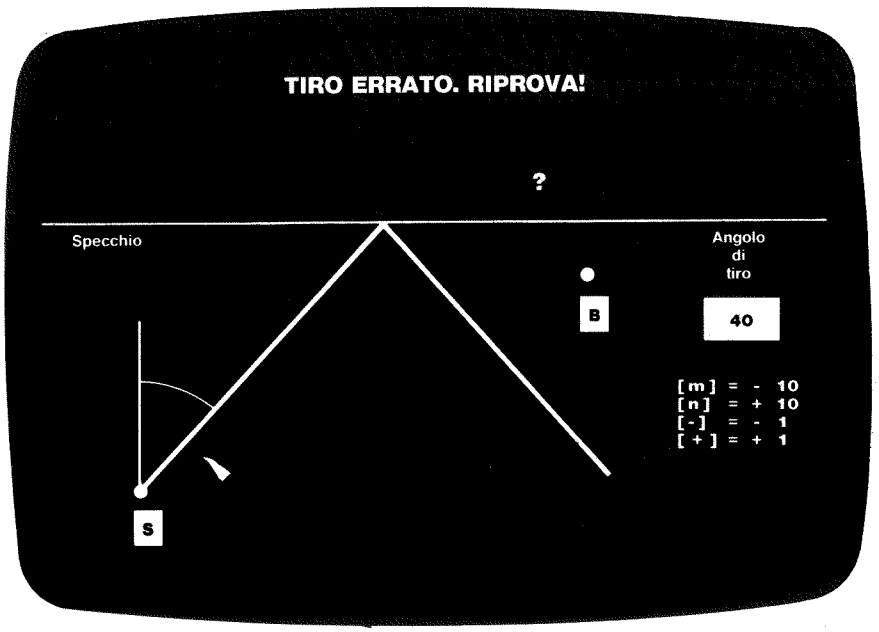


Fig. 3b - Esempio di tiro errato. Lo studente aggiusterà l'angolo di tiro in base alle informazioni visive tratte da questo quadro (nel caso specifico dovrà aumentare l'angolo di tiro).

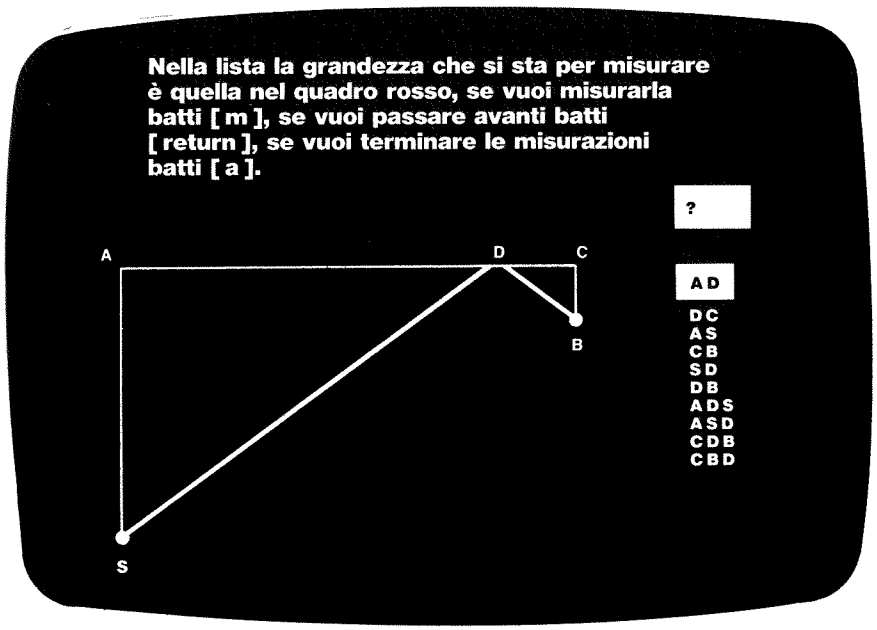


Fig. 3c - Fase di misurazione. Lo studente sceglie cosa misurare (ADS, ASD, CDB, CBD sono angoli) e i dati ricavati vengono immagazzinati in una tabella.

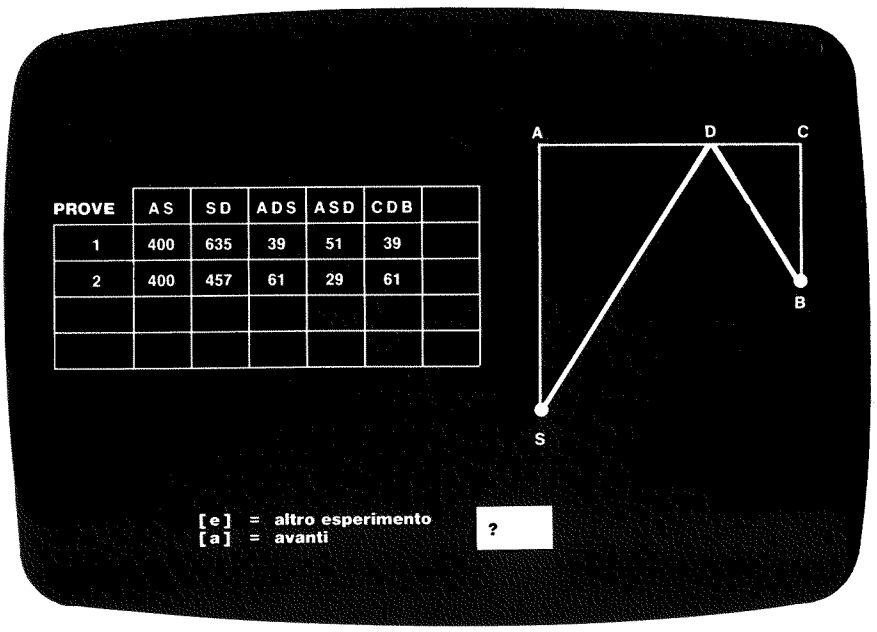


Fig. 3d - Tabella finale con i dati ricavati da una serie di esperimenti. Lo studente a questo punto, osservando i dati, deve poter scoprire la legge; se non vi riesce può chiedere un aiuto al programma.

Fig. 4a - Inizio della simulazione dell'esperimento sulla rifrazione. Lo studente posto in S deve colpire B tenendo conto del fatto che una volta arrivato in 0 il raggio di luce non prosegue nella direzione originaria, ma devia.

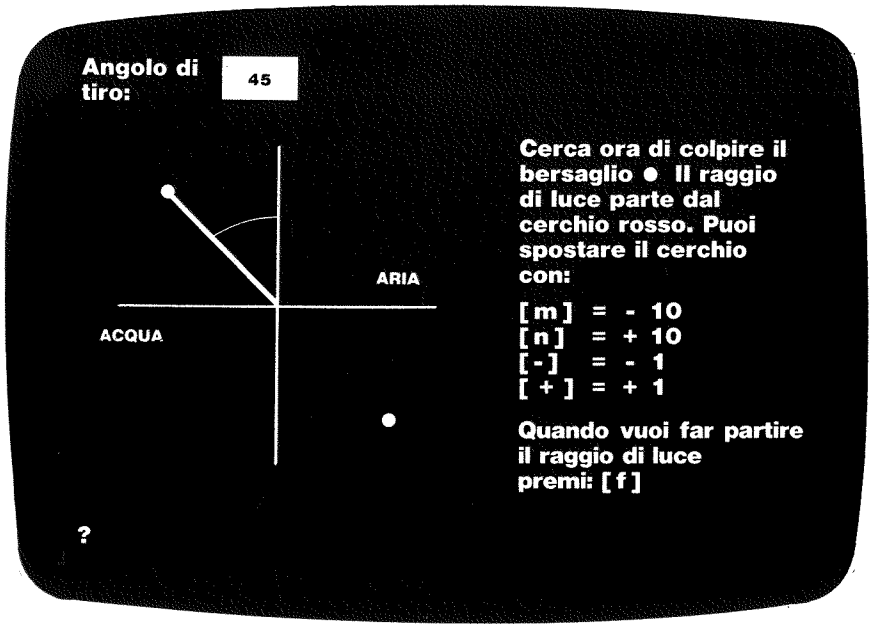
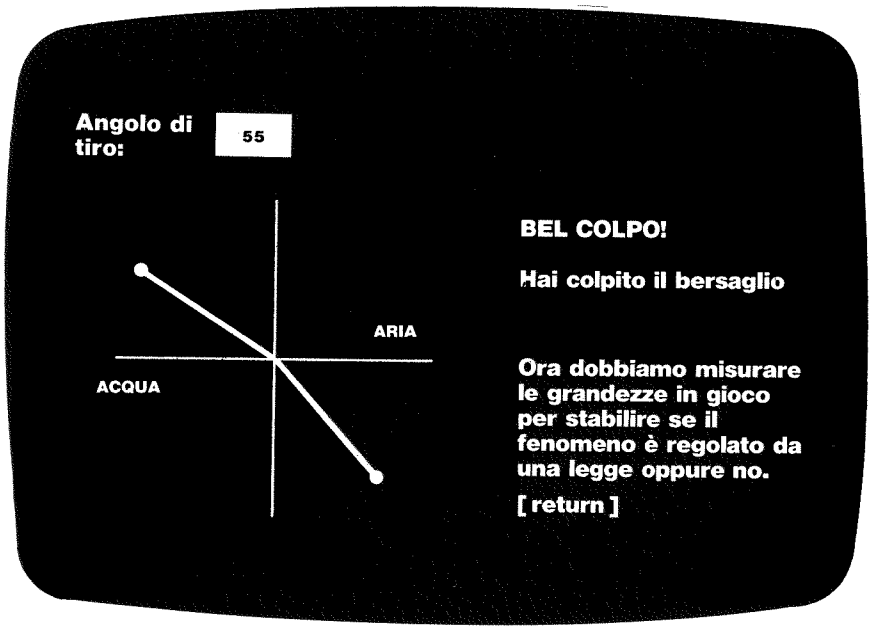


Fig. 4b - Esempio di tiro esatto.



Dopo la prima misurazione vengono eseguiti altri esperimenti (fino ad un massimo di 4) al fine di raccogliere dati da inserire nella tabella; quindi viene presentata la tabella.

Ora lo studente viene invitato ad osservare i dati raccolti e ad estrapolare da questi dati una regola che spieghi il fenomeno. Solitamente le situazioni possibili a questo punto tre: a) lo studente non ha scelto nella misurazione i dati occorrenti al fine di ricavare la regola (nel caso specifico i dati importanti sono gli angoli), b) lo studente ha scelto di misurare le grandezze che servono ma non sa riconoscere la regola, c) lo studente riesce a trovare la regola.

Ovviamente, a seconda dei casi, il programma dovrà comportarsi in maniera diversa. Nel primo caso lo studente viene invitato a ripetere gli esperimenti misurando le grandezze utili; nel secondo caso si suggerisce allo studente di esaminare meglio alcune colonne della tabella e, se ancora non riconosce la regola, viene data la soluzione; nel terzo caso il modulo fa un breve riassunto della legge scoperta e poi termina.

Il terzo capitolo tratta il fenomeno della rifrazione della luce; l'obiettivo di questa parte della lezione è di far scoprire allo studente la legge che regola tale fenomeno.

Questo obiettivo viene ragiunto in varie tappe. Si comincia col far vedere allo studente che quando un raggio di luce passa da un mezzo ad un altro mezzo cambia direzione. Dopo questa prima fase in cui si osserva il fenomeno, come nel modulo precedente, viene presentata una fase di gioco (sempre del tipo "tiro al bersaglio"), in cui lo studente deve utilizzare la variazione di direzione del raggio di luce per colpire un bersaglio (anche in questo caso esiste una routine che permette di cambiare l'angolo di incidenza) (fig. 4a).

Quando il bersaglio viene colpito (fig. 4b), il programma, al contrario

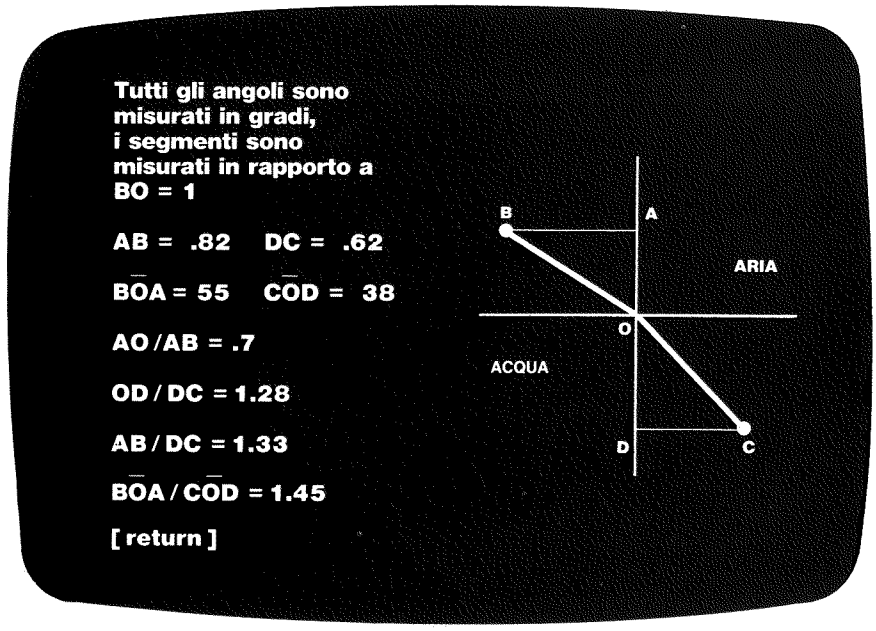


Fig. 4c - Fase di misurazione. Il programma comunica allo studente le misure fatte su una serie di grandezze scelte dal programma stesso. Questi dati vengono immagazzinati in una tabella.
[AB = sen (AOB), DC = sen(DOC)]

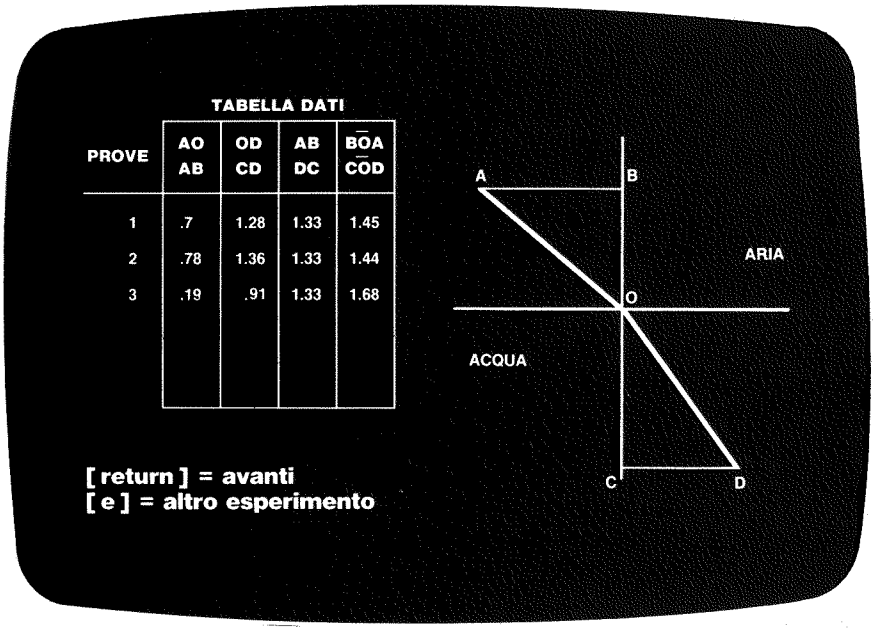


Fig. 4d - Tabella dati. Lo studente può osservare che AB/DC rimane costante; in seguito il programma lo guiderà a scoprire da dove deriva questa costante.

Fig. 4e - Introduzione del concetto di indice di rifrazione.

di quanto avveniva nel modulo precedente dove era lo studente a decidere cosa misurare, si incarica di misurare una serie di grandezze e mette questi valori in una tabella.

Dopo aver ripetuto l'esperimento un certo numero di volte (al massimo 5), viene visualizzata sullo schermo la tabella contenente i dati raccolti, e il programma provvede a far scoprire allo studente una parte della legge della rifrazione. Infatti nella tabella rimane costante il valore della colonna che fornisce il rapporto tra il seno dell'angolo di incidenza e il seno dell'angolo di rifrazione. (Nel caso di studenti che non abbiano studiato la trigonometria, il rapporto, anzichè tra i seni dei due angoli, viene fatto tra AB e DC) (fig. 4c).

Il passo successivo consiste nell'introduzione del concetto di "indice di rifrazione". Viene mostrata una tabella che collega la velocità della luce in un certo mezzo con un numero, detto appunto indice di rifrazione del mezzo; questo numero non è altro che il rapporto tra la velocità della luce nel vuoto e la velocità della luce nel mezzo (fig. 4e).

A questo punto vengono cambiati i mezzi con cui si erano fatti i primi esperimenti; viene ripetuto il gioco del tiro al bersaglio con i due nuovi mezzi, vengono di nuovo rilevati i dati e infine visualizzata la tabella. Viene fatto notare allo studente come il rapporto dei due angoli (angolo di incidenza e di rifrazione), pur rimanendo costante al variare della posizione del bersaglio, non ha lo stesso valore che aveva quando la coppia di mezzi era diversa da quella attuale. Viene quindi visualizzata una nuova tabella il cui scopo è di far scoprire la relazione esistente tra il rapporto tra i seni dei due angoli e gli indici di rifrazione dei due mezzi presi in esame (fig. 4f).

Lo studente, osservando questa nuova tabella, deve scoprire la legge completa che regola il fenomeno della rifrazione della luce. Se vi riesce, il modulo termina con un riassunto della legge stessa; se invece lo studente non riesce a trovare la legge, può chiedere un aiuto al programma o al limite la soluzione. L'aiuto consiste nella possibilità di compiere operazioni elementari (+ − x :) sui due indici di rifrazione, per trovare la relazione tra questi e il rapporto tra seno dell'angolo di incidenza e seno dell'angolo di rifrazione.

Il capitolo di esercizi è l'ultimo della lezione e consta di 4 tipi di esercizi.

Il primo riguarda l'argomento velocità della luce.

Vengono estratte a sorte due distanze (A-B e C-D) ed ognuna delle due distanze viene spezzata casualmente in due parti. Quindi, ad ognuno dei quattro segmenti ottenuti viene abbinato, mediante estrazione, un mezzo preso da una lista di cinque (aria, acqua, quarzo, vetro, diamante). A questo punto viene chiesto allo studente di battere sulla tastiera quale delle due distanze, A-B o C-D, verrà percorsa in minor tempo da un raggio di luce.

Quando lo studente ha fatto la sua scelta, vengono fatti partire due raggi, uno da A e uno da C, così che si possa vedere come vanno in realtà le cose.

Il secondo esercizio riguarda invece la riflessione ed è abbastanza semplice, in quanto consiste solo nel calcolare ad occhio come verrà riflesso da uno specchio un certo raggio di luce. Viene infatti presentato un quadro con una sorgente di luce S, un bersaglio B, un raggio di luce che parte da S ed arriva sullo specchio in un punto 0; lo studente deve decidere se, dopo la riflessione in 0, il raggio colpirà o meno il bersaglio B (il bersaglio viene ovviamente messo in posizione casuale).

Il terzo esercizio riguarda la rifrazione ed è di tipo qualitativo, in quanto si propone di verificare quale associazione mentale lo studente ha fatto tra la deviazione più o meno accentuata del raggio ed il mezzo che l'ha causata.

Infatti l'esercizio presenta una situazione di questo genere: due mezzi uno sopra l'altro, una sorgente di luce, un raggio di luce uscente da questa sorgente con una certa angolazione, l'angolo rifratto corrispondente (fig. 5a).

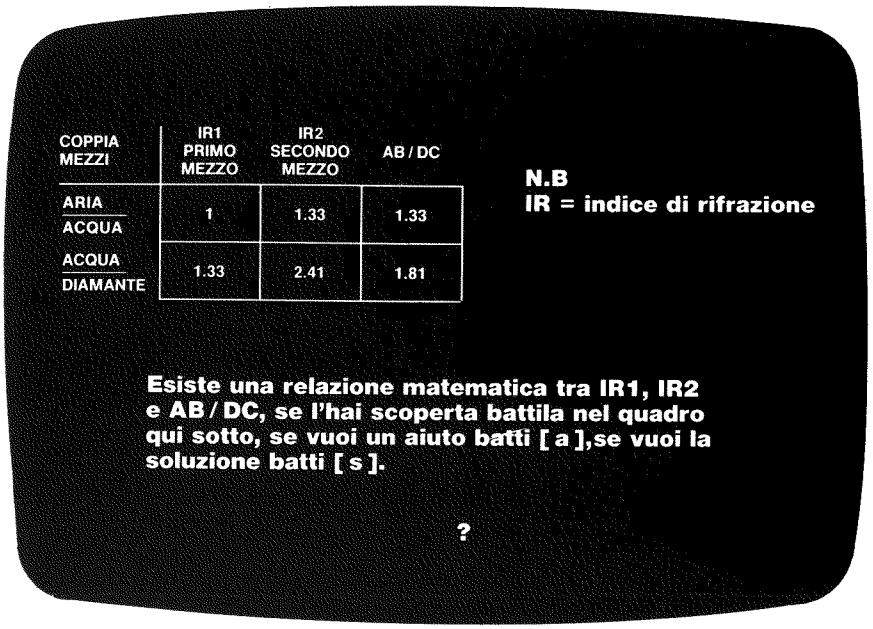


Fig. 4f - Tabella finale. Lo studente, dopo aver fatto altri esperimenti cambiando la coppia di mezzi, dopo aver osservato che AB/DC, pur rimanendo costante al variare dell'angolo di tiro, dipende dalla coppia di mezzi scelti, possiede ora tutti gli elementi per scoprire la legge della rifrazione. Se non riesce a trovare la relazione tra IR1, IR2 e AB/DC può chiedere aiuto al programma.

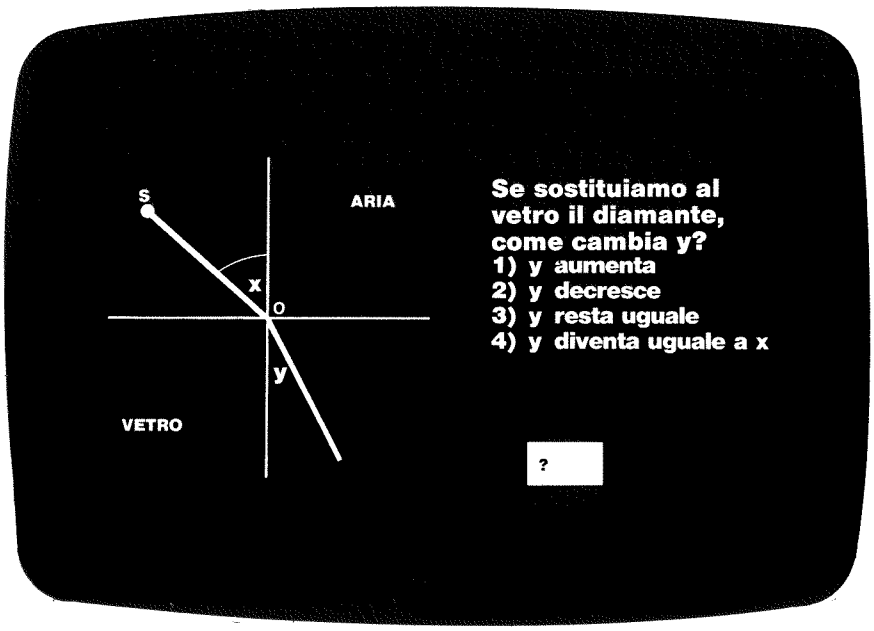


Fig. 5a - Esercizio sulla rifrazione. Lo studente deve dire come varia l'angolo y al variare del secondo mezzo (dal vetro si passa al diamante).

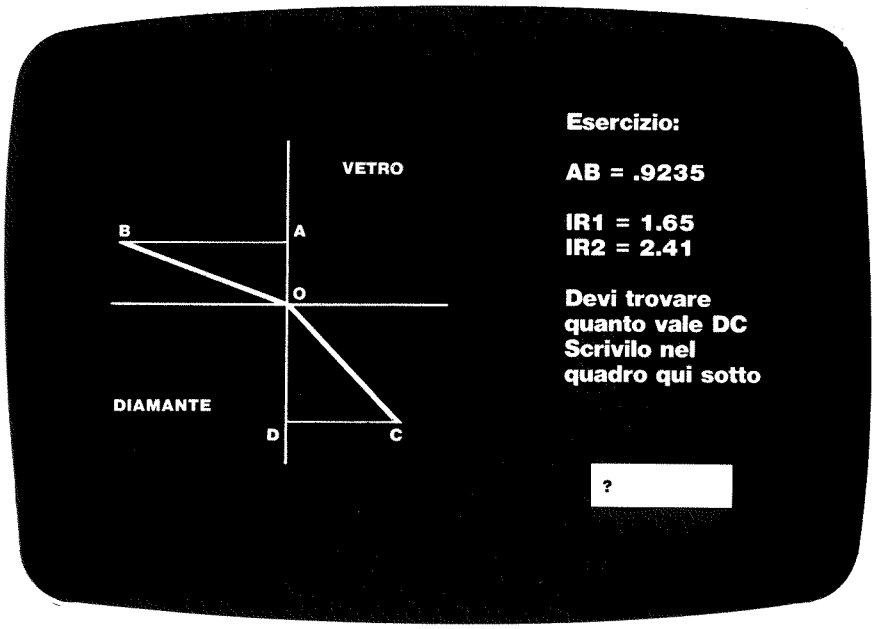


Fig. 5b Esercizio sulla rifrazione. Lo studente applicando la legge scoperta deve trovare la grandezza incognita (DC).

	Tempo	Riflessione	Rifrazione	Esercizi
coppie	1 h. 20	66% A 33% B 0% C	33% A 66% B 0% C	67% D
singoli	1 h. 10	25% A 50% B 25% C	50% A 25% B 25% C	70% D

Fig. 6 - Risultato dei test effettuati con un gruppo di studenti. Gli studenti lavoravano sia a coppie che isolati. I simboli A, B, C, D indicano rispettivamente:
A = studenti che hanno scoperto la legge al primo tentativo
B = studenti che hanno scoperto la legge dopo aver consultato la sequenza di aiuto
C = studenti che hanno richiesto la legge al programma.
D = studenti che hanno risolto gli esercizi.

A questo punto viene cambiato il secondo mezzo e lo studente deve saper dire se il nuovo angolo di rifrazione sarà più grande o più piccolo o se resterà uguale. Al solito, dopo che lo studente ha dato la sua risposta, viene visualizzata la situazione reale e lo studente può vedere se la risposta era esatta o errata.

Il quarto ed ultimo esercizio riguarda ancora il fenomeno della rifrazione, ma affronta l'argomento dal punto di vista quantitativo, nel senso che viene richiesta allo studente l'applicazione della legge scoperta nel terzo modulo e di calcolare, mediante questa legge, l'incognita del problema (fig. 5b).

Le grandezze in gioco sono quattro: i due indici di rifrazione, AB e DC.

A tre di queste quattro grandezze vengono assegnati dei valori estratti a sorte, mentre una rappresenta l'incognita; lo studente, mediante l'applicazione della legge, deve trovare il valore della grandezza incognita.

5. Sperimentazione del programma

Il programma è stato sperimentato da un gruppo di studenti dell'Istituto Tecnico Cannizzaro di Rho (MI), con risultati riassunti nella fig. 6.

Un primo dato è il tempo totale impiegato dagli studenti per seguire la lezione. In media, ogni studente è rimasto davanti al video circa 75 minuti; nonostante il 90% degli studenti abbia indicato nel questionario che la durata della lezione è ragionevole, essa è probabilmente eccessiva per un'unica sessione di lavoro. Un indice di ciò può essere il fatto che l'80% degli studenti abbia indicato i primi due capitoli come i preferiti; probabilmente gli ultimi sono stati seguiti con minor attenzione.

Nella seconda e terza colonna della tabella possiamo vedere, in percentuale, quanti studenti hanno scoperto le leggi al primo tentativo, quanti con l'aiuto del programma e quanti hanno chiesto la soluzione.

Possiamo ritenere i risultati abbastanza soddisfacenti; ad esempio, nel caso di studenti a coppie, nei capitoli chiave nessuna coppia ha dovuto ricorrere alla soluzione presentata dal programma. Anche i risultati del capitolo di esercizi sono piuttosto buoni, se si tiene presente che gli studenti l'hanno affrontato alla fine della lezione, senza quindi poter assimilare meglio le conoscenze acquisite.

Una annotazione interessante riguarda la diversa fruizione tra coppie e singoli: le coppie impiegano un tempo leggermente superiore in quanto discutono molto sulle scelte da compiere; i singoli decidono invece più velocemente, ma in questo modo commettono più errori e sono costretti a perdere poi del tempo per rifare l'esercizio o rispondere di nuovo alle domande.

Al termine della lezione è stato proposto agli studenti un questionario per raccogliere le loro impressioni, le difficoltà incontrate, i loro suggerimenti.

Circa l'80% ha dichiarato di aver avuto problemi nell'uso della tastiera; questo problema si dovrebbe risolvere facilmente con un breve addestramento preliminare sull'uso del computer.

La seconda annotazione interessante riguarda il giudizio dato dagli studenti sull'esperimento; tra gli aggettivi proposti in una lista, sono stati scelti: dal 25% l'aggettivo "divertente", dal 35% l'aggettivo "utile" e dal 40% l'aggettivo "interessante".

Quasi tutti gli studenti hanno sottolineato nei commenti liberi come la lezione risultasse molto più coinvolgente di quelle tradizionali. Inoltre, il 70% userebbe ancora volentieri il calcolatore per altre lezioni, il 20% lo userebbe ancora ma con la presenza del professore, il 10% lo userebbe solo se obbligatorio.

6. Conclusioni

La sperimentazione effettuata ha fornito utili elementi di verifica sul ruolo didattico del computer.

Se si sfruttano opportunamente le capacità di interazione, di grafica, di simulazione offerte dallo strumento, esso può aprire effettivamente nuovi spazi alla didattica.

In particolare, esso può contribuire al coinvolgimento dell'allievo e a renderlo parte attiva nel processo di apprendimento.

7. Ringraziamenti

Si desidera ringraziare per la loro collaborazione:

il Centro di Tecnologie Didattiche del CNR di Genova, ed in particolare il dott. A. Chioccariello,

l'Istituto Tecnico Cannizzaro di Rho (MI), ed in particolare la prof. F. Minnaja.

8. Bibliografia

[1] A. BORK, *Learning with computers,* Digital Press, Bedford, Mass. 1981

[2] V. MIDORO, M. FERRARIS, G. OLIMPO, *Il Computer nella didattica,* SEI, Torino 1985

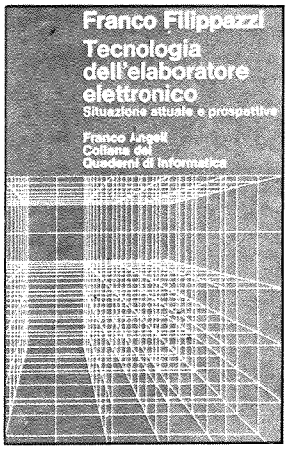
[3] A. BORK, *Production Systems for Computer-Based Learning,* da Instructional software: principles and prospectives for design reviews, Wadsworth Publishing Company, 1984

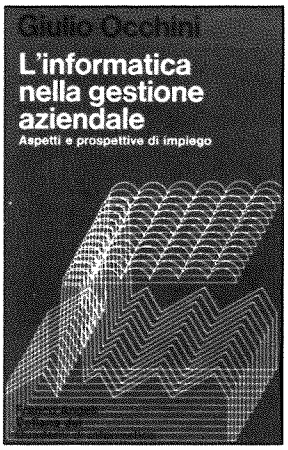
[4] A. CHIOCCARIELLO, G. OLIMPO, G. SPADACCINI, E. SASSI, *Production of a CAL package: a set of criteria and an example in the field of electric circuits,* da "Proceedings of the fourth Canadian Symposium on instructional technology", Winnipeg, Canada, 1983.

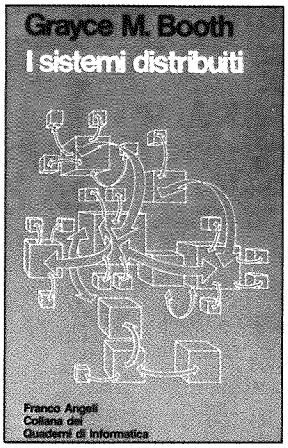
[5] G. GARAVAGLIA, *Progettazione ed implementazione di una unità didattica CBT,* Tesi Università degli Studi di Milano, 1987.

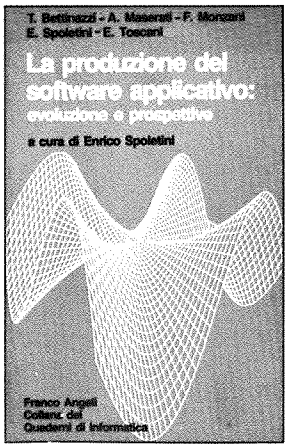
Collana dei Quaderni di Informatica

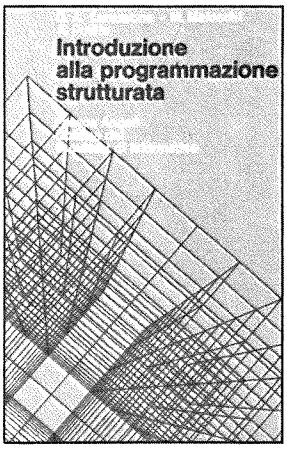
La collana di testi "Quaderni di Informatica" rappresenta la proiezione sul piano librario della presente rivista. La direzione scientifica della collana (che è edita da F. Angeli) è del "Centro Studi Informatica e Automazione" della Honeywell Bull Italia. A titolo di rassegna sintetica, riproduciamo qui di seguito le copertine dei volumi finora usciti, che coprono alcune delle più importanti aree dell'informatica.

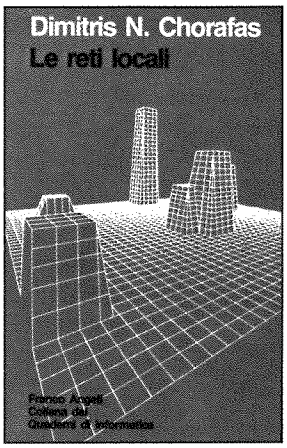


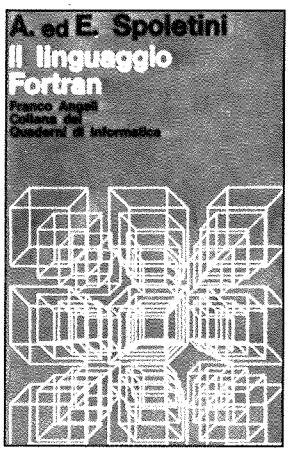


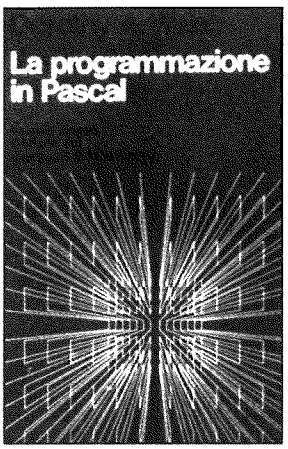












BIBLIOTECA NOVITÀ

Franco Filippazzi, Giulio Occhini: Le frontiere dell'informatica - Vol. I - Edizioni del Sole/ 24 Ore 1986 (L. 28.000).

Il computer è una macchina che si differenzia da tutte le altre perché opera in una dimensione — il trattamento dei simboli e della conoscenza — che attiene alla sfera intellettiva dell'uomo. Non è quindi uno strumento passivo nelle mani di chi lo usa, ma costituisce un formidabile agente di cambiamento del suo modo di operare. Chiunque opera con responsabilità in campo economico, politico, sociale ha dunque la necessità di capire quali sono i fondamenti concettuali di questa disciplina, le sue prospettive di evoluzione, le sue potenzialità applicative. Tale necessità trova però un ostacolo nella letteratura disponibile che oscilla tra due estremi: la divulgazione superficiale e l'ermeticità specialistica. Oltre a ciò, il materiale è di norma frammentario e risulta difficile al lettore orizzontarsi e costruirsi quella visione di insieme di cui ha bisogno. Quest'opera, suddivisa in due volumi — il primo dedicato agli aspetti tecnologici e sistemistici, il secondo alle potenzialità applicative emergenti — vuole essere una risposta a tale esigenza. Essa offre, infatti, una panoramica essenziale e organica della materia con una esposizione che, pur rigorosa, sia accessibile ai non specialisti: opinion maker, manager, professionisti, ricercatori e, in generale, uomini di cultura. Più che al presente, l'opera è rivolta al futuro, delineando le linee di tendenza e i potenziali sviluppi: come saranno le macchine di domani e quali le loro applicazioni sull'arco temporale degli anni Novanta.
Gli autori sono due noti esperti del settore, responsabili delle attività del «Centro Studi Informatica e Automazione», una struttura della Honeywell Bull Italia creata per condurre o coordinare ricerche sugli orientamenti di fondo dell'informatica e della automazione.

Spedizione in abbonamento postale a tariffa intera/Milano